Steffen Augsberg,
Petra Gehring (Hg.)

# *Datensouveränität*

## Positionen zur Debatte

campus

Datensouveränität



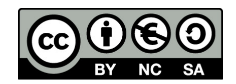
*Steffen Augsberg* ist Professor für Öffentliches Recht an der Justus-Liebig-Universität Gießen. *Petra Gehring* ist Professorin für Philosophie an der Technischen Universität Darmstadt. Beide leiteten im Jahr 2021 gemeinsam die Projektgruppe »Datensouveränität« am Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI). Das Zentrum wird gefördert durch die Hessische Ministerin für Digitale Strategie und Entwicklung.

Steffen Augsberg, Petra Gehring (Hg.)

# Datensouveränität

## Positionen zur Debatte

Campus Verlag
Frankfurt/New York




ISBN 978-3-593-51643-1 Print
ISBN 978-3-593-45194-7 E-Book (PDF)
DOI 10.12907/978-3-593-45194-7


Umschlaggestaltung: Campus Verlag GmbH, Frankfurt am Main.
Satz: le-tex xerif
Gesetzt aus der Alegreya
Druck und Bindung: Beltz Grafische Betriebe GmbH, Bad Langensalza
Beltz Grafische Betriebe ist ein klimaneutrales Unternehmen (ID 15985–2104-1001).
Printed in Germany

www.campus.de

# Inhalt

# Datensouveränität als Diskursgegenstand: Ambiguität als Chance?

*Steffen Augsberg und Petra Gehring*

Unter den »Bedingungen der automatischen Datenverarbeitung« gebe es kein »belangloses« Datum mehr. Diese schlichte, aber ungeheuer bedeutsame und folgenreiche Feststellung trifft das Bundesverfassungsgericht schon 1983 in seinem Volkszählungsurteil (BVerfGE 65, 1, 44). Sie hat durch die Entwicklungen der vergangenen vier Jahrzehnte mehr als nur Bestätigung erfahren. Heute entstehen Daten überall. Und die Möglichkeiten ihrer »automatischen« Verarbeitung sprengen das Vorstellungsvermögen. Technische Fortschritte tragen dazu bei, dass Daten in einer Menge, Diversität und Geschwindigkeit erfasst, verarbeitet und namentlich miteinander verknüpft werden können, die nicht nur das Wissen, sondern auch den Alltag transformiert. Der digitale Wandel wurde zuletzt unter den Schlagworten »Big Data« und »Internet der Dinge« verortet. Inzwischen verbindet man ihn stark mit Innovationen aus dem Kontext sogenannter Künstlicher Intelligenz. Die Fülle der tatsächlichen Entwicklungen stellt dabei offensichtlich traditionelle Schutzmechanismen in Frage.

Das Kompositum Daten-Souveränität reagiert hierauf. Es bildet, das ist unsere Grundthese, gerade deshalb einen interessanten Untersuchungsgegenstand, der zukünftige Entwicklungen potentiell produktiv anleiten und begleiten kann, weil keine Einigkeit darüber besteht, was genau mit dem Wort gemeint ist.

Zwar transportiert der Ausdruck »Datensouveränität« (*data sovereignty*) einige traditionsreiche Assoziationen. Es handelt sich aber um einen recht jungen, erst seit relativ kurzer Zeit öffentliche Diskussionen (mit-)prägenden Terminus. Auch deshalb werden mit dem Begriff durchaus unterschiedliche Zielvorstellungen verbunden; sowohl hinsichtlich der Grundausrichtung wie der Detailliertheit der Vorgaben bestehen teils erhebliche Unterschiede (im Überblick: Hummel u. a. 2021b). In wissenschaftlicher Perspektive neigen wir dazu, dies als Problem zu werten: Unschärfe spricht, wo üblicherweise Präzision angestrebt wird, gegen die Verwendung eines

Begriffs. Auch im öffentlichen Raum wird die Uneindeutigkeit von Begrifflichkeiten gemeinhin als zu bewältigende Herausforderung verstanden. Sowohl aus philosophischer wie aus juristischer wie aus journalistischer Sicht gilt begriffliche Klarheit als Qualitätsmerkmal.

Gleichwohl besteht in allen genannten Feldern auch ein Bewusstsein dafür, dass gerade Begriffe, die festgefahrene Diskurslagen aufschließen, dieses Ideal nicht nur ausnahmsweise, sondern regelhaft verfehlen. Eine gewisse Vagheit, Interpretationsoffenheit und sogar Streitbedürftigkeit von Begriffen ist in vielen Konstellationen – und zwar aus Sachgründen – unvermeidbar. Sie entspricht zudem auch einer Offenheit von Diskurslagen in die Zeit hinein: In der Auseinandersetzung um (neue) Begriffe wird ein Stück Zukunft verhandelt. In diesem Sinne sprechen wir hinsichtlich des Gegenstandes dieses Buches von »Ambiguität als Chance«.

Mit der allgemeinen Einsicht in die potenziell produktive Seite der Vagheit sogenannter Schlüsselbegriffe ist indes noch keine Aussage darüber getroffen, ob der (Daten-)Souveränitätsbegriff diesen Voraussetzungen genügt. Im Gegenteil könnte ja gerade die Tatsache, dass es sich um einen in unterschiedlichen Kontexten bereits eingeführten und mit spezifischen Bedeutungen belegten Begriff handelt, gegen eine Übertragung in andere Sachzusammenhänge sprechen. Von daher rekapitulieren wir zumindest ganz knapp einige philosophische und rechtliche Verwendungszusammenhänge und Begriffsverständnisse, insoweit Anschlussmöglichkeiten, aber auch Abgrenzungserforderlichkeiten bestehen. In den zehn Beiträgen, die dieser Band versammelt, findet sich weiteres reichhaltiges Material hierzu.

Als Herausgeber formulieren wir außerdem Anregungen für ein weiterführendes Nachdenken über den Begriff Datensouveränität. Unsere Thesen zielen nicht darauf ab, eine übergreifende, einheitsstiftende und mit eindeutigen Konsequenzen verbundene Definition zu entwickeln – im Gegenteil erscheint uns gerade das (partielle) Offenhalten gegenstandsadäquat. Im Sinne eines Problemaufrisses wollen wir aber verdeutlichen, vor welcher Hintergrundfolie die nachfolgenden, stärker auf Einzelaspekte fokussierten Beiträge des Bandes entstanden sind. Ebenso möchten wir deutlich machen, dass die hier versammelten Positionen etwas verbindet und warum sie als Teil einer fortlaufenden, wichtigen und in grundlegender Weise sinnvollen Debatte zu verstehen sind.

## 1. Souveränität als Topos politischer Philosophie

In der politischen Philosophie zählt die Souveränität spätestens seit Jean Bodin und Thomas Hobbes zu den zentralen Leitmotiven des sich formierenden Rechtsstaatsdiskurses (vgl. im Überblick: Kelsen $^{2}$1928: 9 ff.). Verstanden wird sie in dieser Tradition meist als nationalstaatsbezogenes Konzept weitgehender Autarkie und unangefochtener Autorität. Im Sinne eines unbedingten Beachtungsanspruchs ließe diese Souveränität sich zwar mit Blick auf einzelne Personen entfalten; typischerweise bezieht sie sich aber auf größere Institutionen. Klassischen Ausdruck findet ein solches, interdependenz- bzw. independenzbezogenes Souveränitätsverständnis in dem überstrapazierten, aber zum Zweck der Pointierung doch hilfreichen Diktum Carl Schmitts: »Souverän ist, wer über den Ausnahmezustand entscheidet.« (Schmitt 1996: 13) – auch hier meint Souveränität eine letztlich als Spitze eines Apparates eher »schaltende« als »waltende« Instanz. Den Ausnahmezustand erklären bzw. beenden zu können, erscheint in dieser Perspektive als Ausdruck weitestgehender Ungebundenheit. Hier bestehen erkennbar Parallelen zu aktuellen Programmen einer sogenannten infrastrukturellen oder auch digitalen Souveränität, die als Debatten über unzulässige Abhängigkeiten von privaten und/oder außereuropäischen Digitaldienstleistern Brisanz und Aufmerksamkeit erhalten. »Die Rede von digitaler Souveränität gleicht dann manchmal einer Beschwörungs- und Beschwichtigungsformel.« (Deutscher Ethikrat 2018: 201) Bestehende begriffliche Überschneidungen sollten allerdings nicht darüber hinwegtäuschen, dass keine echte Kongruenz zwischen digitaler und Datensouveränität vorliegt.

Interessant ist das Schmitt-Zitat zumal aufgrund einer begriffsbezogen weiterführenden Modifikation, die es durch Odo Marquard erfahren hat: »Vernünftig ist, wer den Ausnahmezustand vermeidet.« (Marquard 1994: 7 und 2000: 107; vgl. auch Hacke 2006: 187) Wäre es demnach auch in Digitalfragen vernünftig, die Frage nach Souveränität gar nicht erst aufkommen zu lassen? Immerhin bliebe auch mit Marquard die Frage wichtig, ob der Ausnahmezustand schon eingetreten ist, man also verpasst hat, ihn zu vermeiden – denn dann könnte es dennoch vernünftig sein, über Souveränität zu diskutieren. Allerdings, und dies lässt die begriffliche Bedeutungsvarianz aufscheinen, wäre das dann ersichtlich ein gänzlich anderes Souveränitätsverständnis, nämlich eines, das tatsächlich der intersubjektiv nachvollziehbaren Rationalität deutlich nähersteht als der Macht.

Auch alltagssprachlich könnten wir uns hier an die Wendung von einem »souveränen Umgang mit« etwas erinnern. Wo wir die Kunst des guten Umgangs mit Herausforderungs- und Überforderungslagen als »souverän« bezeichnen, schwingen weder Appelle an den Nationalstaat mit noch die Assoziation, es gehe um zentrales, einsames Entscheiden. Wir sehen also: Souveränität ist ein politischer, kontextabhängiger Begriff, der potentiell (mindestens) zwischen diesen beiden, stärker absolut bzw. stärker relativ ausgestalteten Polen changiert.

»Der Souverän« besitzt allerdings auch für Herrschaftsbegründung eine besondere Bedeutung. Hierfür stehen die vielen Konzepte einer »Volkssouveränität«, die sich im Sinne einer Kraft der Vielen und als Kraft »von unten« als die eigentlich tragende Größe von Staatlichkeit erweist – und auch Geltung zu verschaffen hat. Jean-Jacques Rousseau, Hannah Arendt, Jürgen Habermas, aber auch das deutsche Grundgesetz stehen für Konzepte einer guten Verfassungswirklichkeit, die gerade von der fortbestehenden und auch unter freiheitlichem Vorzeichen kontinuierlich immer neu ausgeübten Souveränität der Bürgerinnen und Bürger lebt. Namentlich im Kontext demokratischer wie rechtsstaatlicher Legitimations- und Legitimitätsdiskurse findet Souveränität in diesem Sinne Verwendung. Dieses Souveränitätsmodell weicht ersichtlich von den vorgenannten Verständnisformen ab. Es lässt sich auch nicht eindeutig in einem binären Schema von einerseits absoluter Macht, andererseits Legitimitätsgrundlage des Rechts verorten, sondern vermittelt gewissermaßen zwischen diesen Positionen, soweit »der demokratische Souverän« sich vor allem in seiner rechtsordnungsgestaltenden und -erhaltenden Funktion verwirklicht (zur Rechtssouveränität siehe Kelsen [2]1928: 22 ff.). Gleichzeitig verweist dieses Souveränitätsverständnis nicht nur auf die Verbindung individueller und kollektiver Legitimationselemente, sondern auch auf eine doppelte, aber nicht immer offengelegte Souveränitätsinanspruchnahme, die wie die Demokratie insgesamt sowohl das einzelne Subjekt wie das Kollektiv erfasst. Zuletzt haben sich im Kontext biopolitischer Analysen in diesem Spannungsfeld die Machtdiagramme verschoben: »Das Problem der Souveränität ist nicht eliminiert; es ist im Gegenteil akuter denn je geworden« (vgl. Foucault 2004: 161). Aus unserer Sicht gilt ähnliches für den Bereich politisch-philosophisch motivierter Analysen von Digitalität.

## 2. Souveränität als Chiffre für verfassungsnormative Grundentscheidungen

Für die juristische Souveränitätsdebatte werden Souveränitätsvorstellungen vornehmlich im Kontext klassischer staats- und völkerrechtlicher Fragestellungen herangezogen, etwa im Streit über Monismus respektive Dualismus (Kelsen [2]1928: 102 ff.). Für Positionierungen innerhalb der Rechtswissenschaft sind diese Aspekte in der Debatte um Datensouveränität jedoch vergleichsweise wenig fruchtbar. Eher lässt sich Datensouveränität im Sinne einer Souveränität des Individuums – diesseits tradierter Terminologien – als eine zusammenfassende Beschreibung spezifischer, verfassungsnormativ primär anders verorteter und separat erwähnter Grundrechtsgarantien verstehen. Das schließt (tages-)politische Beeinflussungen dazugehöriger Debatten nicht aus, setzt den Souveränitätsbegriff aber auch nicht schlicht dem Spiel unterschiedlicher Interessen aus, sondern verweist auf differenzierte, mehr oder weniger voraussetzungsreiche Gestaltungs- und Begrenzungsmöglichkeiten.

Den Ausgangspunkt bildet dabei zwangsläufig die normhierarchisch den anderen Verfassungsvorgaben vorgeordnete Menschenwürdegarantie. Deren genaue Reichweite und Schutzgehalt sind zwar notorisch umstritten. Einigkeit dürfte aber darüber bestehen, dass sie die Grundvorstellung einer zumindest auch subjektiv determinierten Lebensgestaltung umsetzt. Ein würdevolles Leben ist mithin eines, das jedenfalls grundsätzlich in Freiheit und Selbstbestimmung, nicht hingegen in vollständiger Fremddominanz geführt wird:

> »Von der Vorstellung ausgehend, dass der Mensch in Freiheit sich selbst bestimmt und entfaltet, umfasst die Garantie der Menschenwürde insbesondere die Wahrung personaler Individualität, Identität und Integrität. Damit ist ein sozialer Wert- und Achtungsanspruch verbunden, der es verbietet, den Menschen zum »bloßen Objekt« staatlichen Handelns zu machen oder ihn einer Behandlung auszusetzen, die seine Subjektqualität prinzipiell in Frage stellt. Die unverlierbare Würde des Menschen als Person besteht hiernach darin, dass er stets als selbstverantwortliche Persönlichkeit anerkannt bleibt.« (BVerfGE 153, 182, 260 f. m.w.N.)

Das bedeutet keineswegs eine realitätsferne Negation tatsächlich existierender Heteronomie. Es verweist vielmehr auf die Bedeutung adaptiver, neuartige Gefährdungen berücksichtigender und gegebenenfalls sogar antizipierender Schutzmechanismen. Das erkennt schon das Volkszählungsurteil:

»Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten.« (BVerfGE 65, 1, 42 f.)

Ein souveräner Umgang mit entsprechenden neuen Technologien ist demnach dadurch gekennzeichnet, dass der Einzelne diesen nicht vollständig und hilflos unterworfen ist, sondern eine gewisse (in ihrem Umfang noch nicht konkret festgelegte) Beeinflussungs- und somit Selbststeuerungsfähigkeit behält. Das Prinzip der Selbstbestimmtheit würde indes überdehnt, wenn man sie im Sinne einer – letztlich ohnehin illusorischen – jederzeitigen Vollkontrolle verstünde. Schon auf dieser basalen, grundrechtlichen Ebene lassen sich deshalb Ansatzpunkte erkennen, die für abgestufte, auch individueller Gestaltung zugängliche Schutzdimensionen sprechen. Bezogen auf vernetzte, durch kontinuierlichen Datenaustausch gekennzeichnete Gesellschaftsstrukturen bedeutet dies, einerseits problematische Aspekte (insbesondere Machtasymmetrien, Missbrauchspotentiale) möglichst genau zu bestimmen, andererseits aber den Betroffenen Entscheidungsoptionen etwa hinsichtlich der Vernetzungsgrade und des Datenaustauschs zu erhalten. In diesem Sinne erweist sich auch Partizipation als Teilaspekt von Souveränität, und zwar sowohl in einer kontrollerhöhenden Dimension, etwa durch modifizierte Einwilligungslösungen und/oder Datentreuhandmodelle (vgl. Hummel u. a. 2021b: 17 ff.; RfII 2020; von Ulmenstein 2020), als auch mit Blick auf freiwillig vorgenommene, begrenzte Kontrollverluste, auf die das Individuum sich aus freien Stücken ganz bewusst einlässt. Beispielsweise kann es durchaus Ausdruck eines souveränen Umgangs mit eigenen Daten sein, diese bewusst anderen zur Verfügung zu stellen (vgl. Hummel u. a. 2018; Hummel u. a. 2019). Auch hier zeigt sich, dass (Daten-)Souveränität nicht jederzeitige Totalkontrolle verlangt, sondern situations- und persönlichkeitsbezogene Anpassungen, wenn nicht fordert, so doch zumindest zulässt.

Von Würde, Freiheit und Selbstbestimmung führt ein direkter Weg zur »Privatheit«. Dieser Ausdruck ist inzwischen – wenngleich er dem angloamerikanischen Rechtsdiskurs entstammt – auch für Datenschutzdebatten in Deutschland zentral. Privatheit bedeutet nicht nur das Vorhandensein letzter, intimitätssichernder Rückzugsräume, sondern verweist zugleich auf die handlungseinschränkenden Effekte fehlender bzw. reduzierter Privatheit, vor allem infolge kontinuierlicher Beobachtung. Freiheitsbe-

schränkende *chilling effects* können selbstredend situationell, individuell, fallbezogen und sogar generationell unterschiedlich ausfallen. Insbesondere ist es vorstellbar, dass länger anhaltende Übung Gewöhnungseffekte erzeugt, die sich in gewisser Weise sogar positiv auf Freiheitsausübung auswirken. Wer das Narrativ vom »Ende der Privatheit« mehr oder weniger schulterzuckend übernimmt, mag tatsächlich weniger empfindlich auf entsprechende Beschränkungen reagieren (»Ist der Ruf erst ruiniert, lebt sich's völlig ungeniert.«). Umgekehrt folgt hieraus aber kein Plädoyer für einen Fatalismus, der selbst weitreichende Privatsphärenbeschränkungen kritiklos akzeptiert. Jedenfalls sollte klar sein, dass Privatheit und Freiheit eng zusammengehören. Wer umfangreiche personenbezogene Daten sammeln, mit anderen Daten kombinieren und auswerten kann, gewinnt damit die Möglichkeit, auf Basis der so gewonnenen Erkenntnisse steuernd (oder auch nur »stupsend«) in unser Leben einzugreifen und uns zu Entscheidungen zu bewegen, die wir ohne diesen fremden »kleinen« Anstoß nicht getroffen hätten. Freiheitsrechtlich relevant sind somit nicht nur klassische Machtausübungen, etwa im Sinne erzwungener Preisgabe persönlicher Daten, sondern zumal subtilere Beeinflussungen von Präferenzen und subliminal-handlungsrelevante Veränderungen der Lebensumwelt. Damit betrifft der Schutz der persönlichen Daten keineswegs nur die Privatsphäre, sondern unmittelbar die Freiheit eigenverantwortlicher Lebensführung. In diesem Sinne leuchtet es unmittelbar ein, das verfassungsrechtliche Konstrukt der informationellen Selbstbestimmung weiterzuentwickeln zu einer sogenannten informationellen Freiheitsgestaltung (Deutscher Ethikrat 2018). Wie weit diese Freiheitsgestaltung kollektiv überformt werden darf oder muss, etwa im Sinne nicht disponibler Schutzstandards, ist damit noch nicht gesagt. Immerhin impliziert aber (auch) diese terminologische Neuorientierung eine erhöhte Sensibilität für Steuerungseffekte und die unterschiedlichen Möglichkeiten, auf diese Einfluss zu nehmen. Und zwar »Einfluss« auch durch aktiven, entscheidungsgetragenen »Einsatz« dessen, was Daten an Machtvektoren eröffnen. In der digitalen Welt lassen sich bürgerliche Freiheiten nicht mehr nur als etwas modellieren, das man mittels Abwehrrechten aus der Welt von Wertschöpfung und Ressourcenkonflikten heraushalten muss, sodass man letztlich meine Daten (die stets nur andere verwerten, während ich sie um den Preis der Einwilligung stets nur weggeben oder allenfalls »spenden« kann) vor mir selber schützt. Womit wir wieder bei der Souveränitätsfrage sind.

## 3. (Daten-)Souveränität als entwicklungsoffenes und Entwicklungen anleitendes Paradigma

Zwar ist mit dem Bezug auf die Souveränität alles andere als eine eindeutige Zielrichtung verbunden. Indes ist, das dürfte nach den skizzierten Entwicklungslinien und Hintergrundannahmen klar sein, die Aussage erlaubt, dass der Begriff der (Daten-)Souveränität Flexibilitäten ermöglicht, die bereichsbezogen mindestens wünschenswert sind. Anders als andere Begriffsübernahmen, namentlich die ähnlich prominente Vorstellung eines Daten-Eigentums (vgl. Thouvenin 2017; Fezer 2017a, 2017b), werden damit zwar Anleihen an bestehenden Verständnissen vorgenommen. Der Begriff ist aber nicht entsprechend verfestigt bzw. mit eindeutigen (Rechts-)Folgen und Voraussetzungen verknüpft. Sektorspezifisch gebotene und gegebenenfalls auch fortlaufende Anpassungen schließt er nicht aus. Damit erweist sich die teilweise kritisierte »Ambiguität« in wirtschaftlicher Hinsicht als Wettbewerbsvorteil, lädt aber auch die Bürgerinnen und Bürger zur aktiven Mitgestaltung neuer Routinen im Umgang mit Daten ein. So wie Innovationsoffenheit schon länger als Qualitätsmerkmal von Institutionen verstanden wird, kann sie sich auch auf die Erfassung und regulatorische Mitgestaltung der Lebenswelt erstrecken. Innovationen profitieren zwar von der durch eindeutige rechtliche Regelungen garantierten Verlässlichkeit. Allzu starre Strukturen und Modelle können aber nicht nur innovationshemmend wirken, sondern kaschieren Machtfragen, die man in einer Demokratie offen diskutieren muss. Namentlich in dynamischen Gesellschaftsbereichen ist in besonderem Maße darauf zu achten, Kreativität nicht zu beschränken, sondern nur in geordnete Bahnen zu lenken und damit zu unterstützen (vgl. Augsberg 2013). Es dürfen eben nicht nur Datenkonzerne bei der Nutzung, Auswertung und teils auch Erschleichung von Daten »kreativ« sein – während sich das technische Gefälle zu Lasten von letztlich nur noch auf dem Papier »geschützten« Bürgerinnen und Bürgern vergrößert. Will informationelle Selbstbestimmung wirklich Selbstbestimmung sein, müssen Grundrechtssubjekte vielmehr neben dem Instrument eines bloßen »Ja« oder »Nein« zur Weggabe von Daten auch Bedingungen an die Verwendung von Daten knüpfen dürfen. Ebenso sind Forderungen nach aktiven Durchsetzungsmöglichkeiten individueller Rechtspositionen im digitalen Raum nicht schon deshalb obsolet, weil dieser nun einmal ein globaler ist.

Datensouveränität sollte sinnvollerweise freilich nicht dazu dienen, bestehenden (Daten-)Schutzmechanismen pauschal ihre Legitimität abzusprechen. Im Gegenteil erinnert der Begriff daran, dass auch an sich gut begründete, tradierte Mechanismen unter neuen Bedingungen funktionale Defizite erleiden können und deshalb (immer wieder) neu überdacht und gegebenenfalls angepasst werden müssen. Beim Ruf nach »Souveränität« kann es nicht darum gehen, jegliche als problematisch empfundene Machtausübungen auszuschließen. Mit der Rückanbindung an die souveräne Lebensführung des Einzelnen wird aber deutlich, dass manipulationsbegrenzende Instrumente und auch Autorisierungen von Einzelnen wie von Kollektiven vonnöten sind. Wenn das EU-Recht neuerdings die Bildung von Datengenossenschaften anregt, dann sehen wir dies als Impuls für »mehr« Datensouveränität. Zu verhindern sind (mindestens) Datenzugriffe, die den Betroffenen die Kontrolle über die Bedingungen ihres Handelns nehmen und damit ihre Selbstbestimmtheit entwerten. Es sind aber auch neue Formen des Zusammenschlusses und des kollektiven Verfügens über Daten zu (er)finden. Angesichts der komplexen Teilhabeansprüche und Kontrollmöglichkeiten des Individuums, aber auch dessen multipler Interaktionen mit zahlreichen weiteren Personen und Institutionen, erscheint es naheliegend, hier regulatorisch eine Multiakteursverantwortung einzufordern und abzusichern (vgl. Deutscher Ethikrat 2018). Das lässt zugleich Raum für etwas anders akzentuierte Schutzkonzepte, etwa ein noch stärker auf die Teilnahme an der Datenwirtschaft rekapitulierendes Verständnis der Datensouveränität »als Ausprägung der Privatautonomie« (vgl. Beise 2021).

Datensouveränität, das zeigt der bisherige Verlauf der Debatte und zeigen auch die nachfolgenden Beiträge, darf jedenfalls nicht als vorübergehendes Modewort missverstanden werden. Eher kann der Begriff als Paradigma, als Indikator spezifischer Herausforderungen sowie als dynamisches Leitkonzept entsprechender umgreifender Gestaltungs- und Regulierungsanstrengungen aufgefasst werden. Die hier versammelten »Positionen« zielen darauf ab. Sie bilden in diesem Sinne keinen Abschluss der Debatte, sondern verdeutlichen – hoffentlich mit Wucht – deren historisch-politische Raumtiefe und ihr produktives Potential.

## 4. Positionen zur Debatte

Zum oben beschriebenen Zweck versammelt der vorliegende Band Beiträge aus Philosophie, Rechtswissenschaft, Wirtschaftswissenschaft, Politikwissenschaft und Theologie. Wir trennen sie bewusst nicht gemäß fachlicher Herkunft, sondern bringen schritt- oder vielleicht auch »schichtweise« unterschiedliche Perspektiven zusammen. Am Ende ergibt sich ein Bild mit Überlagerungen, denn tatsächlich ist unser Gegenstand mehrdimensional. Entsprechend konzipieren wir unseren Sammelband als Durchlesebuch. Die Beiträge verweisen vielfach auch aufeinander.

Mit begrifflichen Unterscheidungen – nämlich dem auf den ersten Blick unübersichtlichen Ineinander der Konzepte »Datensouveränität« und »digitale Souveränität« – befasst sich zunächst *Petra Gehring*. Ihr zufolge hat man es in Genese und Verlauf rund um die beiden Schlagworte trotz vielerlei Vermischungen nicht mit einer, sondern mit mehreren Debatten zu tun. *Wolfgang Kerber und Karsten K. Zolna* entwickeln aus ökonomischer Sicht in Bezug auf die komplexen Marktversagensprobleme bei der Sammlung und Nutzung von Daten auf digitalen Märkten einen Datensouveränitätsbegriff, der sich aus dem in der verbraucherpolitischen Diskussion wohletablierten Konzept der Konsumentensouveränität ableitet und sich mit aktuellen datenpolitischen Diskussionen konkret verknüpfen lässt. Es bleiben jedoch Zweifel an den bisherigen Ansätzen zur Lösung solcher Probleme, sodass (neue) regulatorische Möglichkeiten in ihrer Gesamtheit bedacht werden müssen. Das Recht ist somit gefordert: *Kevin Ferber* beleuchtet die informationelle Selbstbestimmung aus Sicht des deutschen Grundgesetzes und der europäischen Grundrechtecharta. Das Grundrecht im Sinne von Datensouveränität zu deuten, hält er für plausibel und möglich. Aus der Perspektive des Datenschutzrechtes zeigt *Anne Riechert* demgegenüber auf, wie differenziert die Betrachtungsweise dennoch sein muss, um einerseits Grundrechten auch weiterhin gerecht zu werden und andererseits Spielräume nicht zu übersehen, über die das Datenschutzrecht ja bereits verfügt. Aktuelle Weiterentwicklungen geben hier Antworten auf das, was hinter dem Ruf nach Souveränität an Bedürfnissen verschiedener Anspruchsgruppen steht. *Florian Möslein und Clara Beise* wählen den Blickwinkel einer als Privatautonomie und also zivilrechtlich ausgestalteten Datensouveränität. Auch diese muss den Schutzgedanken nicht verabschieden, legt aber den Akzent auf Handlungs- und Verfügungsfreiheiten, die das Rechtssubjekt und konkret das Individuum innehat. *Steffen Augsberg* vergleicht mit Daten-

schutz, Datensouveränität und Data Governance drei unterschiedliche (und unterschiedlich stark konzeptionell ausgearbeitete) Regelungsansätze und führt sie auf spezifische Grundansätze zurück. Im Ergebnis bedeutet dies ein Plädoyer für Kontextorientierung und wechselseitige Inspiration statt trennscharfer Abgrenzung. Mit der in der deutschsprachigen politischen Theorie derzeit kritischen Sicht auf die Datensouveränität – nun wieder dezidiert: als Begriff – befasst sich *Tim Eckes*. Er zeigt, wie man es auf der Linie der politischen Philosophie von Hannah Arendt keineswegs bei einer Ablehnung der Rede von der »Souveränität« in der Digitalpolitik belassen muss. Vielmehr sind auch Aspekte einer Datensouveränität »mit Arendt« zu gewinnen. *Jan C. Schmidt und Stefan Gammel* schließen an Diskussionslinien zur Technikgestaltung an, um die Datensouveränität in ihrer Mehrdeutigkeit ebenfalls letztlich »politisch«, nämlich als Sache von Partizipation zu verorten. Mit der erstaunlich klar gefassten Datensouveränitäts-Definition des europäischen Dateninfrastrukturprojektes Gaia-X setzen sich *Christian Person und Moritz Schütrumpf* in ihrem Beitrag auseinander, der dabei auch Einblicke in die Ziele und in aktuelle Entwicklungsstände von Gaia-X gibt. Neben der Diskursebene und derjenigen marktlicher und rechtlicher Dispositive zeigt sich im Blick auf Gaia-X auch so etwas wie eine infrastrukturelle Ebene, auf welcher die »Souveränität«, und sei es als Metapher, Entwicklungspotenziale freizusetzen scheint. Mit seinem Beitrag zu »Datentoxikalität« bietet abschließend *Gerhard Schreiber* einen durchdachten, neuen und originären Blickwinkel an, unter welchem der digitale Wandel datenethisch, vielleicht aber auch im Sinne einer Art Datenökologie neu verstanden werden kann. Denn auch in dieser (letztlich globalen) Hinsicht stellt sich die Frage, wie »souverän« wir angesichts der Ubiquität von Daten sein können, wenn also – obwohl Daten nicht verschwinden – die Gesellschaft sich gänzlich der Maxime von immer mehr Digitalität verschreibt.

# Datensouveränität versus Digitale Souveränität: Wegweiser aus dem konzeptionellen Durcheinander

*Petra Gehring*

»Souveränität« ist rund ums Digitale in aller Munde, das steht fest. Der Begriff ist in der öffentlichen Sphäre dabei überwiegend positiv besetzt. Dies dürfte in Europa keineswegs nur darauf zurückzuführen sein, dass die EU-Kommissionspräsidentin von der Leyen in ihrer Rede zur Kandidatur im Juli 2019 unter dem Agenda-Punkt »Europe fit for the Digital Age« Anstrengungen für mehr »technologische Souveränität« für Europa angekündigt hat.[1] Im September 2020 konkretisiert sie dann weitere Punkte von »Europe's digital sovereignty on a small and large scale« (Von der Leyen 2020: 8). Die deutliche Spitze gegen von außerhalb Europas agierende marktbeherrschende Konzerne hat zwar sicher in ein bereits vorhandenes Bild gepasst: Europa ist von den USA und China sowie von weiteren großen Digitalmächten abhängig.

Dennoch geht die Attraktivität der Rede von Datensouveränität nicht ohne Weiteres auf eine Vision aus Brüssel zurück, Europa solle digital unabhängiger sein. Auch sind es keineswegs nur Netz-Nerds, die der Datensouveränität das Wort reden, der digitalen Souveränität, der technologischen Souveränität, der Plattformsouveränität. Eher ist das Gegenteil der Fall. Der Wunsch danach, »souverän(er)« zu sein, fällt gerade auch bei an digitalen Zugzwängen resignierenden Verbrauchern, bei überforderten kleinen und mittelständischen Unternehmen, bei den Betroffenen von Cyber-Attacken und bei denjenigen, die sich ihre vielen Passwörter nicht mehr merken können, auf fruchtbaren Boden. Vor allem aber evoziert der Ruf nach Souveränität den Gedanken an Recht und Gesetz: weniger nach strengerem Recht als nach Rechtsdurchsetzung überhaupt. In hohem Maße werden digitale Räume als anarchisch erlebt, und was globale Netzgemeinschaften als Frei-

1 »It may be too late to replicate hyperscalers, but it is not too late to achieve *technological sovereignty* in some critical technology areas.« (Von der Leyen 2019: 13).

heit feiern, erleben längst viele Menschen als Niederlage des Rechtsstaates, dessen Bürgerinnen und Bürger sie sind: Man will kein unfreies Netz. Man will sich aber auch nicht zynischen Geschäftsmodellen ausliefern, maschinengenerierter Pseudo-Information oder einem anonymen Mob. Es gibt also womöglich so etwas wie ein Syndrom des Überfordertseins, auf welches der Diskurs um Souveränität im Digitalzeitalter – dem Stand des digitalen Wandels heute – reagiert. Feierten die libertären Netzdebatten der 2000er Jahre die Schwäche des Staates und deuteten sie diese als auch demokratischen Befreiung, wird Digitalisierung heute vermehrt als Schwächung gewählter Demokratien und insbesondere als Entwertung von Recht im klassischen Sinne – der Publizität und Nachvollziehbarkeit von gemeinschaftlich gewollten, legitimierten Regeln sowie von Rechtssicherheit und Rechtsdurchsetzung – erfahren.

Diese Intuitionen lassen sich aus meiner Sicht belegen durch die kurze, aber komplexe Verschränkungsgeschichte der Begriffe »Datensouveränität« sowie »digitale Souveränität« und zwar im Blick speziell für den deutschsprachigen, als einem primär in Europa situierten Diskurs. Was meint »Datensouveränität« und was demgegenüber »digital souverän«? Beide Begriffe tauchen fast gleichzeitig auf – nachfolgend Belege ab 2013. Beide Begriffe sind umstritten und vor allem gehen beide Begriffe (einschließlich kritischer Unterstellungen, die gleichsam von dem einen auf den anderen überspringen) auf teils groteske Weise durcheinander. Sie werden dabei verwechselt, krass gegensätzlich gelesen und akzentuiert – und sie scheinen mir auch ein durchaus auf »Kommunikationsblasen« verteiltes, separiertes Eigenleben zu führen.

Ob dies generell das Schicksal politisierter Kunstworte ist, ist eine große Frage, die den Rahmen dieses Aufsatzes übersteigt. Jedenfalls aber lassen sich bestimmte Verdachtsmomente wie auch Fehllektüren der beiden Begriffe durch eine Rekonstruktion ihrer Geschichte entkräften. Man tut zudem gut daran, beide Konzepte nicht zu vermengen, sondern erstens präzise zu fassen und zweitens damit dann auch – was ihrer Genese entspricht – sie hinreichend klar zu unterscheiden. Dies festhaltend komme ich am Schluss meines Beitrages auf meine eingangs angedeutete, vor allem rechtspolitische, aber auch die Frage der Macht in digitalen Wirklichkeiten betreffende Diagnose zur Aktualität beider Begriffe – der Daten- und der digitalen Souveränität und damit der Souveränitätsfrage überhaupt zurück. Um diesen großen Bogen schlagen zu können, wird nachfolgend zunächst an die lange Begriffsgeschichte von »Souveränität« ganz generell erinnert.

## 1. Souveränität – eine Großvokabel

In jedem Lehrbuch zur politischen Theorie wird rekonstruiert, wie mit Bodin und Hobbes zunächst ein säkulares Staatsverständnis entsteht: Der »Souverän« ist, schematisch gesprochen, gesetzgebungs- und entscheidungsbefugter Herrscher, dem auch die Ausübung der Staatsgewalt – gegebenenfalls »absolut«, sogar *legibus solutus*, losgelöst vom geltenden Recht – zusteht. Rückblickend werden gern die absolutistischen Wurzeln des Souveränitätskonzepts betont. Gleichwohl sind gerade auf der (mit Hobbes beginnenden) Linie vertragstheoretischer Vorstellungen von legitimer politischer Machtausübung die vielfältigen Konzepte einer »delegated power from the people« (Locke 1689/90 II, § 149) und dann, wuchtiger, einer »Volkssouveränität« für Europa wie in der angelsächsischen Welt bestimmend geworden. Die *Virginia Bill of Rights* von 1776 formuliert den Gedanken, die französische Menschenrechtserklärung von 1789 prägt die dann zur Grundnorm moderner Demokratien gewordene Formel: »Le principe de toute souveraineté réside essentiellement dans la nation«.[2] Dass in dieser Tradition etwa Art. 20 des deutschen Grundgesetzes (wie schon die Verfassung von Weimar) postuliert, »alle Staatsgewalt« gehe »vom Volke aus«, ist bekannt.

Vor diesem gefestigten demokratietheoretischen Hintergrund kann das abstrakte Konzept Souveränität gleichwohl Unterschiedliches akzentuieren: zum einen die Unabhängigkeit des Entscheidens, die Macht eines monolithischen Souveräns, eines »Tyrannen« gar, noch diesseits jeglicher rechtsstaatlichen Legalität, zum anderen das genaue Gegenteil, nämlich gerade die Autorisierung von Recht durch diejenigen, welche auf der Legitimität der Verfassung bestehen – und die von daher jeder rohen Gewaltausübung das Recht sowie politische Partizipationsverfahren entgegensetzen. Vor allem in radikalliberaler Perspektive und wohl besonders in angelsächsischen Debatten steht der Souveränitätsgedanke für zentralistische Herrschaft und *Law and Order*. In demokratietheoretischen Kontexten hingegen und wohl namentlich in der politischen Öffentlichkeit Europas gehört der Souveränitätsbegriff zum Inventar einer vertrauten und vertrauenswürdigen Form, die abgeleitete – im Kern vor allem prozedurale – Legitimität der Rechtsstaatlichkeit pluralistischer Gesellschaften zu beschreiben. Dass Rechtsstaatlichkeit nicht bedeutet, dass das Recht selbst »souverän« ist,

---

2 Ich zitiere hier nach Quaritsch 1995: 1107.

bleibt dabei klar. Vielmehr bleiben der verfassungsgemäße Gesetzgeber nicht des einzelnen Gesetzes, sondern im umfassenderen Sinne als Schöpfer und Garant der »Rechtsordnung« (Kelsen $^{2}$1960: 31 ff.) sowie konkret auch die Gerichte, wenn sie die Gesetztheit von Normen bestätigen (Kelsen 1979: 114), einem prozeduralen Verständnis von politischer Legitimität verpflichtet. Dieses schließt auch alle anderen Verfassungsorgane sowie die durch die Verfassung instituierten und geschützten öffentlichen Austausch- und Aushandlungsprozesse mit ein. Wie immer man den Rechtsstaat definiert: In der Perspektive demokratischer Souveränität darf das Recht weder von Politik »aufgesaugt« noch von ihr »abgespalten« werden (vgl. Habermas 1992, $^{5}$1995: 584).[3] Diese Sichtweise beinhaltet auch – in vor-digitalen Zeiten eigentlich eine Selbstverständlichkeit –, dass eine vollständige Technisierung des Rechts der Idee der Volkssouveränität (wie auch der Souveränität der Demokratie) widersprechen würde. Automatisierung des Rechts – und sei es nur der Rechtsausübung und -durchsetzung – stünde politischer Selbstbestimmung entgegen. Nicht nur umfasst das Urteilen stets den Blick auf den konkreten Einzelfall, der mittels Leitgrößen wie Verhältnismäßigkeit, Angemessenheit, Billigkeit und nicht zuletzt der Kunst von Schlichtung und Vergleich weit mehr ist als die bloße Applikation eines Schemas. Sondern Recht setzt letztlich einen frei gefassten politischen Willen um, es muss auch von daher in einem bürgerschaftlich glaubwürdigen Sinne bis in die Umsetzung hinein eine Handlung sein. Maschinellem Entscheiden sind daher enge Plausibilitätsgrenzen gesetzt, jedenfalls in der Justiz und überall dort, wo die Rechtswirklichkeit von Spielräumen lebt.

Ein Feld, in welchem »Souveränität« nochmals anders konnotiert ist und auch von der Demokratiefrage wegführt, ist das Völkerrecht. Hier werden mit Konzepten wie »territorialer Souveränität«, der Souveränität im Luftraum oder hinsichtlich der Verwertung von Bodenschätzen formale Merkmale – oder auch Minima – autonomer Staatlichkeit begrifflich konserviert, wie sie, wenn man so will, seit dem 16. Jahrhundert Thema sind.

3 Wie man das nennt, was das Verhältnis von Recht und Politik, wenn sie demokratisch wechselseitig »Medium« füreinander sein sollen, denn nun eigentlich stabilisiert, ist eine weithin offene Frage. Naturrechtler und Diskursethiker halten hier die »Verschränkung« beider »mit Moral« (Habermas 1992, $^{5}$1995: 585) für entscheidend. Nachfahren vormoderner Markttheorien setzen auf die Konvergenz von »Interessen«, komplexere sozialwissenschaftliche Konzepte sehen Systemrationalitäten sowie Technisierungseffekte (»Verfahren«), politische Philosophien in der Tradition Foucaults ein analysebedürftiges Zusammenspiel von Wissensregimes und sich historisch wandelnden Machtformen (nebst »Mikrophysik«) am Werk.

Hier meint Souveränität schlicht »Hoheit«, und zwar primär Hoheit nach außen. Es geht also um zwischenstaatliche Verhältnisse, um die Abwehr von Ein- oder Übergriffen und um die Intaktheit von Grenzen. Ähnlich spricht man von Souveränität auch dort, wo staatliche Herrschaft gerade nicht mehr in der Lage ist, Grenzen aufrechtzuerhalten und zu sichern – nämlich im Fall des Souveränitätsverlusts. Gleichsam nach »innen« gerichtet betrifft dies auch die Frage bzw. den Fall der Sezession: Dort, wo territoriale Einheiten oder Populationen sich für unabhängig erklären, wird auf der einen Seite eine existierende souveräne Einheit verletzt, auf der anderen Seite eine souveräne Entität neu behauptet. Und vielleicht dann auch – in der Moderne idealtypisch: in selbstbestimmter Weise – neu gegründet.

Festhalten lässt sich: »souverän« ist ein in hohem Maße politisches Attribut. Es mobilisiert sowohl Vorstellungen der Ordnungsstiftung und der Ordnungsmacht als auch ein Pathos von Freiheit und Selbstbestimmung. Medium der Souveränität sind Gewalt, Politik und die Rechtsform gleichermaßen – und darin, dass diese drei Elemente abstrakt zusammenkommen, nicht in der Person des Herrschers oder im »Volk« selbst, sondern allenfalls in seinem Votum oder seiner Entscheidung, liegt der Witz des Begriffs. Bezüglich des Machtvektors, den er impliziert (*top down*? *bottom up*? horizontal?) ist der Souveränitätsbegriff neutral. Ebenso kann man »souverän« bestehende Ordnungen/Grenzen stabilisieren oder aber neue Ordnungen/Grenzen etablieren.

Allerdings lenkt die Frage nach »Souveränität« stets aus der bloßen Zone der routinierten Regelanwendungen heraus. Der Begriff hat Pathos. Er rückt die »rohe« Dimension des Schaffens, Sicherns und Legitimierens (und also die Gewalt wie die Fragilität) von Ordnung in politische Diskurse zurück.

## 2. Datensouveränität: Verfügen über persönliche Daten

Wirft man, die politische Philosophie im Hinterkopf haltend, einen Blick auf die frühen Vorkommen des Ausdrucks »Datensouveränität«, so wird deutlich, wie wenig wir es hier mit den geschilderten Zusammenhängen zu tun haben. Ganz deutlich steht hier nämlich das Individuum im Fokus. Es geht um individuelle Freiheitsansprüche der Person, genauer: des einzelnen Marktteilnehmers und Bürgers. Und zwar in Kontexten, die auf Verbraucherschutz sowie auf das spezifisch deutsche Grundrechtskonstrukt des sogenannten »allgemeinen Persönlichkeitsrechts« (durch höchstrichter-

liche Rechtsprechung abgeleitet aus Art. 2 und Art. 1 GG) und dem hieraus wiederum abgeleiteten Recht der »informationellen Selbstbestimmung« verweisen. Allerdings scheint »Datensouveränität« als eine Art Individualrecht, das zugleich aber Entscheidungsmacht und persönliche Kontrolle mit umfassen soll, in eine interessante Spannung zum Datenschutz geraten.

So schreibt das Bundeswirtschaftsministerium der vorletzten Bundesregierung in seiner *Digitalen Strategie* 2016, eine der frühen Belegstellen des Begriffs:

»Die digitale Transformation der Gesellschaft erfordert einen Paradigmenwechsel in der Datenpolitik. Daten sind der zentrale Rohstoff der digitalen Wirtschaft. Immer mehr, immer feinere und differenziertere Dimensionen von Wirtschaft und Gesellschaft werden gemessen und verwertet, vernetzt und vermarktet. Die Vermeidung von Datenerhebung und Datenerfassung kann nicht länger unsere Leitlinie sein. Vielmehr geht es in Zukunft um Datensicherheit und um individuelle ›Datensouveränität‹.« (BMWi 2016: 33)

Der nächste Absatz umschreibt den angekündigten »Paradigmenwechsel«, es solle darauf verzichtet werden, Datenerhebung zu vermeiden, jedoch aber gehe es künftig um Sicherheit und (gewahrte? oder sogar geschaffene?) Souveränität:

»Bürgerinnen und Bürger sowie Unternehmen müssen darauf vertrauen können, dass ihre Daten gegen Missbrauch geschützt sind. Nutzer und Verbraucher müssen souveräne Entscheidungen über die Verwendung ihrer Daten treffen können. Datensicherheit und Datensouveränität sind wichtige Grundpfeiler unserer Demokratie und zugleich Voraussetzung für die Akzeptanz und den Erfolg einer datengetriebenen Ökonomie.« (Ebd.)

Datensouveränität im Sinne »souveräner Entscheidungen« der Nutzer und Verbraucher über »die Verwendung ihrer Daten«. Mit der »Datensicherheit« sei sie wichtiger »Grundpfeiler unsrer Demokratie« wie auch für Voraussetzung einer künftigen »datengetriebenen Ökonomie«: Die Stoßrichtung dieser Formulierungen ist klar. Der »Datenschutz« fehlt, er wird durch das Duo Souveränität und Sicherheit ersetzt. »Souverän« schütze ich mich allenfalls nun selber. Der datenschutzrechtliche Grundsatz der sogenannten Datensparsamkeit (das Gebot, unnötige Datenerfassung zu unterlassen) wird mit der Forderung, Datenerhebung nicht länger zu vermeiden, sogar geradewegs für obsolet erklärt.

Wie der Neuling namens »Datensouveränität« »entwickelt« werden soll, erläutert das Papier freilich kaum. Einleitend heißt es, man solle diese Souveränität »sichern« (BMWi 2016: 8), wie Datensicherheit sei sie ein »Prinzip« (vgl. ebd.: 26), und es wird angekündigt, »Datensouveränität und Da-

tenschutz« sollten durch Überarbeitung des Datenschutzrechts an neue Geschäftsfelder angepasst werden (vgl. ebd.: 23).

Wenig überraschend haben Datenschutzrechts-Expertinnen und -Experten sowie namentlich die Datenschutzbehörden der deutschen Bundesländer auf diese Signale sofort und auch heftig reagiert. In einem Papier *Grundsatzpositionen und Forderungen für die neue Legislaturperiode* fordert im Jahr 2017 die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, »das Verbotsprinzip nach der DSGVO nicht durch den Anspruch auf ›Datensouveränität‹ aufzuweichen«; bei der begrifflichen Neuerung handele es sich um

»ein Schlagwort in der politischen Auseinandersetzung um die zeitgemäße Positionierung des Datenschutzes, das in unterschiedlichen Zusammenhängen gebraucht wird. Aus der Alltagssprache entnommen, wird der aus dem Staatsrecht stammende Begriff ›Souveränität‹ mit selbstbestimmtem Handeln assoziiert, der einen Anspruch auf (absolute) Herrschaft über die eigenen persönlichen Daten beinhaltet. Dies allerdings kommt nach gegenwärtigem Rechtsverständnis allenfalls im Kernbereich privater Lebensgestaltung in Betracht. Zudem trifft er datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern.« (Datenschutzkonferenz 2017a: 1)

Der politischen Absicht hinter dem – mit falschen Assoziationen aus dem Staatsrecht die Bürger über ihre Rechte irreleitenden – Begriff, denn allenfalls ganz privat sei man ja souverän, tritt das Papier entgegen:

»Die DSK spricht sich daher dafür aus, auch künftig das aus der Menschenwürde abgeleitete Recht auf informationelle Selbst-bestimmung in den Mittelpunkt zu stellen und bei dem funktionalen Begriff des datenschutzrechtlichen Verbotsprinzips zu bleiben.« (Datenschutzkonferenz 2017a: 1)

Ähnlich formuliert es eine ebenfalls 2017 verabschiedete »Göttinger Erklärung« der Datenschutzkonferenz, *Vom Wert des Datenschutzes in der digitalen Gesellschaft*. Datenschutz werde von politischer Seite immer häufiger »als Hindernis diskreditiert«, es befremde sehr,

»wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

›Datensouveränität‹ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.« (Datenschutzkonferenz 2017b: 1 f.)

Datensouveränität – nämlich vielleicht gar der Einstieg in eine persönliche »Verwertungshoheit« der Bürger als Eigentümerinnen und Eigentümer, die ihre Daten in Eigenregie vermarkten, mindestens aber ein Kontrollversprechen, das den angesichts digitaler Machtasymmetrien so wichtigen Schutzgedanken preisgebe – sei ein »Kampfbegriff« für »anderen (= weniger) Datenschutz« (Hansen 2021: 8).

Ein Zwischenresümee aus rechtswissenschaftlicher Perspektive lautet:

»Aber auch in Deutschland und dem sonstigen Europa gibt es immer wieder Versuche, unter Schlagworten wie ›Dateneigentum‹ oder ›Datensouveränität‹ neue Ideen in der Debatte zu verankern, von denen nicht immer klar ist, ob sie – z. B. durch eine Hinzunahme vertragsrechtlicher oder ökonomischer Argumente – erstens die im datenschutzrechtlichen Sinne betroffenen Personen stärken, zweitens nicht womöglich deren Rechte gerade umgekehrt zugunsten ökonomischer Verwertungsinteressen schleifen oder drittens lediglich innerhalb des datenschutzrechtlich vorgegebenen Rahmens neue Abwägungsargumente liefern und außerhalb dieses Rahmens (d. h. für anonyme Daten) rechtliche Zuordnungskriterien liefern wollen. [...] Gerade die Versuche, eine Ökonomisierung des Datenschutzes zu erreichen und das Prinzip ›Dienst gegen Daten‹ zu etablieren, verkennt aber die Zwecke des Datenschutzes und seine Bedeutung für eine freiheitliche Gesellschaft und zur Verhinderung von Machtmissbrauch auf der Basis überlegener Information [...].« (Simitis/Spiecker gen. Döhmann/Hornung 2019: 310)

Tatsächlich hat schon 2014 der Rechtsanwalt und Fraunhofer-Projektleiter im Bereich Intelligente Systeme unter Verweis auf den Datenbedarf von Big-Data-Anwendungen ein »Grundrecht auf Datensouveränität« gefordert. Das deutsche Datenschutzrecht sei nicht praxistauglich und »im Ergebnis technologieunterlegen«, der Bürger sei nicht »Herr seiner Daten« (vgl. Seidel 2014: 154 f.).

»Da das informationelle Selbstbestimmungsrecht das anvisierte Ziel eines Datenherrprinzips nicht erreichen konnte, bedarf es einer ergänzenden Neuausrichtung, bei der der

einzelne Bürger nicht mehr nur als zu schützender Regelungsadressat, sondern auch als persönlicher Regelungsakteur berechtigt wird, über die Nutzung und Verwendung seiner Daten innerhalb eigenständiger Souveränitätsspielräume zu verfügen und verbindliche Einzelfallregelungen zu treffen.« (Seidel 2014: 153)

Der Einzelne sei im Rahmen des geltenden Datenschutzkonzepts, in welchem »nur die betrieblichen und behördlichen Stellen über das missbrauchsanfällige Datenpotential verfügen«, fixiert »auf seine Funktion als Datenobjekt« (ebd.). Seine provokativ vorgetragenen Forderungen ergänzt Seidel mit dem Hinweis darauf, den von ihm lediglich erweiterten Begriff »Datensouveränität« hätten in den 2000er Jahren Datenschützer, und zwar mit Blick auf Löschungsrechte angesichts der damals geplanten elektronischen Gesundheitskarte, selbst aufgebracht (vgl. ebd.: 155).

Im Kern geht es Seidel – jenseits der offenkundigen industriepolitischen Nutzenkalküle – darum, neben dem »Alles oder Nichts« der Einwilligung dem Einzelnen auch für eigene ökonomische Nutzenkalküle aktive (eigene) Verfügungsrechte über Daten und Datenspuren einzuräumen, es bedürfe eines »wirtschaftlich *eigentumsähnliche[n] Recht[s]* am eigenen Datum«, eines »utilitär geprägten Selbstbestimmungsrechts« (Seidel 2014: 158) – und zwar auch, um die »Datenmacht zwischen datenverarbeitenden Stellen und datenbetroffenen Individuen« (ebd.) neu zu ordnen. Derzeit stünden für eine erfolgreiche Regulierung des »freiheitszersetzende[n] wie auch [...] freiheitsentfaltende[n] Potential[s] des exponentiellen Datenwachstums«, so die gesetzgebungspolitische Alternative, »[d]er Datenschutz für den permanent gläserner werdenden Bürger und der von der Rechtsordnung zu befähigende Bürger als Regisseur seiner persönlichen Sachverhaltskonstrukte« (ebd.: 159) einander gegenüber. Den Vorwurf einer mit der vorgeschlagenen erweiterten Datensouveränität einhergehenden Individualisierung nimmt Seidel zustimmend vorweg: Die vorgeschlagene Neuerung verkörpere in der Tat »die Entwicklung von der egalitären Massenfalldemokratie hin zu einer *diversitären Einzelfalldemokratie*« (ebd.: 165).

Den Gedanken der Eigenregie greift, wenn auch behutsam und ohne Bezug auf die 2017 dann schon entflammte Debatte, der Deutsche Ethikrat in seiner ebenfalls 2017 beschlossenen (2018 publizierten) Empfehlung zu Big Data im Gesundheitssystem erneut auf. Nun wird das Konzept Datensouveränität als »verantwortliche informationelle Freiheitsgestaltung« beschrieben und damit an den – dem Datenschutzrecht ja zugrundeliegenden – Verfassungsbegriff der informationellen Selbstbestimmung rhetorisch angenähert:

> »*Datensouveränität*, verstanden als eine den Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung, sollte das zentrale ethische und rechtliche Ziel im Umgang mit Big Data sein.
>
> Der Begriff der informationellen Freiheitsgestaltung knüpft an das Konzept der informationellen Selbstbestimmung an, entwickelt dieses aber weiter. Eine solche Freiheitsgestaltung gründet nicht in einem eigentumsanalogen Ausschlussrecht; vielmehr geht es wesentlich um die Befugnis, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt und sich dadurch kommunikativ entfaltet. Informationelle Freiheitsgestaltung in diesem Sinne meint interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt.« (Deutscher Ethikrat 2018: 252)

Der Rat vermeidet die Rede von eigentumsähnlichen Rechten oder auch von volkswirtschaftlichem Nutzen, deutet aber sowohl die Potenziale individueller Datenverwertung als auch einen Gemeinschaftsnutzen (»Daten als soziale Ressource«) an:

> »Mit dem Begriff der *Datensouveränität* wird […] die Absicht betont, den souveränen, also selbstbestimmten und verantwortlichen Umgang des Einzelnen mit seinen eigenen personenbezogenen Daten mit einer Realisierung der Potenziale zu verknüpfen, die Big Data sowohl gesellschaftlich als auch für die individuelle Lebensgestaltung eröffnet. Daten müssen nicht allein als wichtiges individuelles Gut verstanden, sondern auch in ihrer kollektiven Dimension verstanden werden. Der Einzelne bleibt maßgeblicher Bezugspunkt von Datensouveränität; darüber hinaus ist aber die Relevanz von Daten als soziale Ressource ebenfalls zu berücksichtigen.« (Deutscher Ethikrat 2018: 253)

Mit einer systematischen Ausdifferenzierung, derzufolge erst vor dem Hintergrund »negativ-protektiver Aspekte von Selbstbestimmung« – sprich: nur auf der Basis von wirksamem Datenschutz – »gehaltvolle Entscheidungen über die eigenen Daten« überhaupt möglich seien (Hummel u. a. 2021a: 7), hat eine Autorengruppe, darunter Mitglieder des Ethikrates, kürzlich umrissen, wie Datenschutz und Datensouveränität vielleicht vereinbar seien könnten. Ökonomische Verwertbarkeit für den Einzelnen wie auch eigentumsartige Rechte, aber auch Aspekte des Gemeinnutzens (etwa von Genomsequenzen) sind in der rechtspolitischen Abwägung. Ebenso sind die Ermöglichung zweckgebundener sogenannter »Datenspenden« oder die Einlieferung in einen Datentreuhänder Gesichtspunkte, die nach vorn treten (solches liegt etwa für gemeinwohlorientierte Zwecke nahe, auf die

auch das entstehende EU-Recht abhebt[4]). Die Verfügung über eigene Daten muss also nicht automatisch eine maximal profitorientierte Vermarktung sein. Dennoch hält die Debatte – als nach wie vor stark an Individualrechten und an die deutsche Grundrechtsjudikatur geknüpfte Kontroverse – an. Von Befürwortern eines klassischen Datenschutzes wird insbesondere geltend gemacht, dass die »informationelle Selbstbestimmung« ja durchaus nicht nur ein negatives Grundrecht sei. Weswegen der Datenschutzgedanke sich auch ohne einen Paradigmenwechsel weiterentwickeln ließe.[5]

## 3. Digitale Souveränität: Kompetenz vs. Rückbau von Abhängigkeiten

Auch die »digitale« Souveränität findet sich in Deutschland als Programmwort schon deutlich früher als die eingangs zitierte Verlautbarung der angehenden EU-Kommissionspräsidentin von 2019, nämlich etwa 2013 in einem Zukunftspapier des IT-Planungsrates der deutschen Länder, das eine digitalpolitische Agenda für die nächsten acht Jahre entwirft. Erneut erscheint »Souveränität« – hier nun: »digitale Souveränität« – als vollständig individuelle Angelegenheit, und zwar diesmal im Sinne einer Kompetenz, die fehle und gefordert wird. Der IT-Planungsrat der Länder buchstabiert dies damals folgendermaßen aus:

> »Digitale Souveränität heißt […] zunächst IKT bzw. digitale Medien sinnvoll bei der Suche, Beurteilung und Verwendung von Daten und Informationen im Internet einsetzen zu können, kompetent mit den eigenen Daten umgehen zu können, Chancen und Vorteile der Digitalisierung zu erkennen und zu nutzen, aber auch sich möglicher Gefahren bei der Internetnutzung bewusst zu sein – sowohl im Hinblick auf den technischen als auch den organisatorischen Umgang.« (IT-Planungsrat 2013: 34)

Digital »souverän« zu sein, meint folglich, fähig zu sein, mit digitalen Lösungen (wie auch Daten) gut und kenntnisreich sowie hinsichtlich möglicher Gefahren auch umsichtig umzugehen. Und diese Fähigkeit ist wie ein Bildungsgut steigerbar:

---

4 Der Data Governance Act (DGA), eine neue EU-Regulation, sieht ausdrücklich die Schaffung »altruistischer« Datenintermediäre vor, die auf der Basis konditionierter Datenspenden Daten »teilen«, also weitergeben oder Datenauswertungen ermöglichen könnten.

5 Aus rechtwissenschaftlicher Sicht ist das Thema noch deutlich komplexer. Siehe hierzu den Beitrag von Riechert in diesem Band.

»Je stärker die Zugangsmöglichkeiten des Einzelnen zur digitalen Welt vorhanden sind, je mehr Wissen und Kompetenz er bei IKT-Themen hat, je häufiger und vielfältiger er digitale Medien nutzt und je offener und reflektierter er mit digitalen Themen und Neuerungen umgeht, desto stärker ist seine digitale Souveränität ausgeprägt.« (Ebd.)

Diese, an ein pädagogisches Lernziel erinnernde Bestimmung wird flankiert von einer nüchternen Diagnose: »In Anbetracht der rasanten Entwicklung der IKT-Medien hinkt die Bevölkerung in ihrer digitalen Souveränität beträchtlich nach; aktuell wird in Deutschland lediglich ein mittlerer Digitalisierungsgrad erreicht.« (IT-Planungsrat 2013: 40) Der Befund mündet in die Handlungsaufforderung an die Politik – und wohl insbesondere an diejenige der in Deutschland für die Bildungs- und Hochschulressorts zuständigen Länder –, dort, wo jenes Wissen und die geforderten Kompetenzen fehlen, nämlich augenscheinlich vor allem »in der Bevölkerung«, digitale Souveränität endlich »aufzubauen«: »Der Aufbau digitaler Souveränität bei allen Bürgerinnen und Bürgern und in allen Unternehmen ist als wichtige politische Aufgabe umzusetzen.« (Ebd.)

Einer so eindeutig als Kompetenz bestimmten digitalen Souveränität stehen Begriffe nahe wie (medienpädagogisch geprägt) »Digitalkompetenz« bzw. »digitale Kompetenz« oder (bibliothekswissenschaftlich geprägt) »Informationskompetenz« sowie derjenige (leicht herablassende) einer – etwa für Senioren angeratenen (vgl. Klug/Große Starmann 2019: 12) – »digitalen Alphabetisierung« (»Digital Literacy«).[6]

Eine Umakzentuierung, für die deutsche Öffentlichkeit vielleicht auch Neuprägung, erfährt das Stichwort »digitale Souveränität« demgegenüber dann im Rahmen des Berichts der Datenethikkommission der Bundesregierung von 2019. Hier wird nun tatsächlich über den Umweg der Figur eines »Datenschutzes für Unternehmen« (als Schutz nicht nur vor dem eigenen Staat, sondern vor der Konkurrenz aus dem Ausland) die zwischenstaatliche Dimension und damit ein ganz anderes – wenn man so will: das klassisch politisch-theoretische – Souveränitätskonzept ins Spiel gebracht. »Stärkung der digitalen Souveränität Deutschlands und Europas« heißt der 10. Leitgedanke des Berichts (vgl. Datenethikkommission 2019: 13), und die unter der Zwischenüberschrift »Für einen europäischen Weg« vorgetragene, einschlägige Überlegung lautet:

6 »Data Literacy«, also datenbezogenes Alphabetisiertsein, heißt die dann wiederum epistemische Vision einer Datenkompetenz aller (nicht nur der informatischen) Fachkulturen, vgl. im Auftrag des »Hochschulforums Digitalisierung« Schüller u. a. 2019.

»Trotz des berechtigten Fokus auf Datenschutz natürlicher Personen darf der Schutzbedarf von Unternehmen und juristischen Personen nicht in den Hintergrund treten. Durch die umfassende Verknüpfbarkeit von Einzeldaten kann ein lückenloses Bild interner Betriebsabläufe entstehen und in die Hände von Konkurrenten, Verhandlungspartnern, Übernahmeinteressenten usw. gelangen. Dies stellt aufgrund umfangreicher Datenflüsse in Drittstaaten u. a. eine Gefährdung der digitalen Souveränität Deutschlands und Europas dar.
Bemühungen um die langfristige Sicherung der digitalen Souveränität Deutschlands und Europas sind daher nicht nur ein Gebot politischer Weitsicht, sondern auch Ausdruck ethischer Verantwortung.« (Datenethikkommission 2019: 32)

Je nach Einsatzgebiet, fächert die Datenethikkommission die zu bedenkenden datenpolitischen Folgeketten an anderer Stelle auf,

»können die Auswirkungen algorithmischer Systeme gesamtgesellschaftliche Relevanz haben, etwa auf die demokratische Willensbildung, die Bürgernähe staatlichen Handelns, auf den Wettbewerb, auf die Zukunft der Arbeit und auch auf die digitale Souveränität Deutschlands und Europas.« (Ebd.: 164)

Allerdings ist der Sprachgebrauch der Datenethikkommission zumindest hinsichtlich des Attributes »souverän« nicht ganz eindeutig, sofern er in seinen Empfehlungen zuweilen auch Formulierungen wählt, die augenscheinlich doch dann wiederum den Bereich der Datensouveränität meinen. Ein Beispiel: »Einzelne Bürger müssen informierte und souveräne Entscheidungen bezüglich der Verwendung algorithmischer Systeme treffen können […]. Auch das ist eine Konsequenz des ethischen Prinzips der digitalen Selbstbestimmung.« (Ebd.: 169)

Informiertes, souveränes Entscheiden Einzelner – an dieser Stelle erhält die datenschutzrechtliche Einwilligung ein wenig den Anstrich des aus der Medizinethik bekannte »Informed Consent«. Und tatsächlich bezeichnet die Datenethikkommission die »digitale Selbstbestimmung« hier quasi im Vorbeigehen ja dann auch als ein weder politisches noch (datenschutz)rechtliches sondern als ein – nun – »ethisches« Prinzip.

Feinheiten wie diese wird man zumeist überlesen. Der »europäische Weg« bleibt das viel deutlichere und das eigentlich wichtige Signal. So gehört es zu den Errungenschaften des Datenethikkommission -Berichts, die Formel von der »digitalen Souveränität Deutschlands und Europas« für die deutsche Debatte mit zu prägen. Dass dies durchaus nicht mit martialischem Unterton geschieht, lohnt sich ebenfalls zu betonen. Denn es ist nicht das Bild der großen Konzerne oder Machtblöcke, gegen die man sich behaupten müsse, das die Datenethikkommission in den Vordergrund

stellt, sowie auch nicht »Deutschland« als handelnde Entität, sondern es bleibt bei einer Semantik der Sorge um die »deutsche und europäische« Unabhängigkeit.

Einen ähnlichen Ton wählt 2020 dann auch die damalige Bundeskanzlerin vor dem europäischen Parlament, wenn sie die »digitale Abhängigkeit von Drittstaaten« zwar erwähnt, dann aber geradezu demonstrativ die Perspektive einer ganz normalen Bürgerin einnimmt (»viele von uns im Verlauf ihrer täglichen digitalen Kommunikation«) und dann auch den »Schutz unserer Demokratien« vor Problemen wie Lüge, Desinformation und Populismus anspricht – Themen also von eigentlich eher innenpolitischer Natur:

»[G]erade auch in den vergangenen Wochen und Monaten ist uns Europas digitale Abhängigkeit von Drittstaaten erneut deutlich geworden. Dies haben viele von uns im Verlauf ihrer täglichen digitalen Kommunikation zweifellos festgestellt – sei es bei der Technologie oder bei den Dienstleistungen. *Es ist wichtig, dass Europa digital souverän wird.* Gerade in den Schlüsselbereichen wie der künstlichen Intelligenz und dem Quantencomputing, aber auch beim Aufbau einer vertrauenswürdigen und sicheren digitalen Infrastruktur wollen wir vorankommen.

Entscheidend ist auch der effektive Schutz unserer Demokratien vor Cyberbedrohungen und Desinformationskampagnen. Denn eine Demokratie braucht eine Öffentlichkeit, in der Wissen und Informationen geteilt werden können und in der sich Bürgerinnen und Bürger austauschen und darüber verständigen können, wie sie leben wollen. Wir erleben es gerade: Mit Lüge und Desinformation lässt sich die Pandemie nicht bekämpfen, ebenso wenig wie mit Hass und Hetze. Dem Fakten leugnenden Populismus werden seine Grenzen aufgezeigt. In einer Demokratie braucht es Wahrheit und Transparenz. Das zeichnet Europa aus […].« (Merkel 2020: 8 f., meine Hervorhebung, PGG)

Digitale Souveränität findet sich hier erstaunlich direkt sogar mit der Frage der Demokratie als Staatsform verbunden. Als Subjekt der Souveränität erscheinen ja weniger Staat und Regierung (oder auch ein der Durchsetzung harrendes Recht) als vielmehr die bürgerliche Öffentlichkeit. »Grenzen« aufgezeigt werden nicht anderen Staaten, sondern einem »Fakten leugnenden Populismus« – sofern dieser den Raum, in welchem Bürgerinnen und Bürger mit dem Ziel der wechselseitigen Verständigung, die auch eine Selbstverständigung beinhaltet, »Wahrheit und Informationen« teilen. Fast scheint es, als habe hier ein Diskursethiker, der die Wendung »digital souverän« in einen neuen, nämlich nicht länger staatsherrschaftlichen, sondern demokratietheoretischen Kontext überführen wollte, der Kanzlerin die Feder geführt.

## 4. Babylonisches Durcheinander: die Datenstrategie der Bundesregierung Anfang 2021

Mögen die Rede von Kommissionspräsidentin 2019 und Kanzlerin 2020 subtile Untertöne haben – wer in Sachen »Datensouveränität« einerseits und in Sachen »digitaler Souveränität« andererseits programmatisch Orientierung sucht mittels der Anfang 2021 veröffentlichten Datenstrategie der Bundesregierung der großen Koalition, geht in einem begrifflichen Wirrwarr verloren.

Die Termini »Souveränität« oder »souverän« kommen inflationär, nämlich insgesamt 33 Mal vor. Und nun werden »Daten-« und »digitale Souveränität« fast beliebig genutzt und auch verwechselt. So heißt die Unabhängigkeit von internationalen Cloud-Dienstleitern nun nicht »digitale«, sondern Datensouveränität:

> »Zur Stärkung der → Datensouveränität europäischer Verbraucherinnen und Verbraucher sowie Unternehmen werden wir technische, rechtliche und institutionelle Lösungen suchen, um den in der Praxis aufwendigen Wechsel von Cloud- Dienstleistern zu erleichtern und → Lock-In-Effekte zu verringern.« (Bundesregierung 2021a: 25)

Das vernetzte europäische Projekt GAIA-X biete eine »sichere und souveräne Dateninfrastruktur« (ebd.: 12) – entweder wohl als Fall von Daten- oder aber technologischer Souveränität, da auch die »technologische Souveränität« weiter »ausgebaut werden« soll (vgl. ebd.: 13). Im Hinblick auf Quantencomputing gelte es »von vornherein auf die Stärkung unserer Souveränität [zu] achten« (vgl. ebd.: 14). Auch wären Datensouveränität (oder doch digitale Souveränität?) aus Europa heraus künftig zu exportieren: »Ferner sollen Datensouveränität und Datensicherheit über die Grenzen Europas hinausgedacht werden. Besonders mit Blick auf unseren Nachbarkontinent Afrika« (ebd.: 26).

Mit Bezug zum Datenschutz wiederum ist nicht mehr nur von individuellem Grundrechtsschutz, etwa Datenschutz durch verbessertes Einwilligungsmanagement (vgl. ebd.: 19), sondern nun auch von »mehr europäischer[r] Datensouveränität« die Rede, also doch wohl eher vom internationalen Wettbewerb der Rechtsräume (und damit von digitaler Souveränität?):

> »Das divergierende Datenschutzverständnis verschiedener Aufsichtsbehörden innerhalb der EU kann ebenfalls Herausforderungen für eine harmonisierte Rechtsanwendung und für mehr europäische → Datensouveränität hervorrufen.« (Ebd.: 17)

Datensouveränität mutiert abseits der Selbstbestimmung zu einer (Daten)*Nutzer*souveränität: »Vertrauen in den sicheren Umgang mit Daten und insbesondere die Stärkung der Nutzersouveränität sind zentrale Elemente zur Förderung innovativer Geschäftsmodelle für die Mobilität. […]« (ebd.: 32) »Souveräne« sowie nicht sichere, sondern »differenzierte« Datenhandhabung und europäische Spielregeln werden gleichgesetzt:

»Daher schaffen wir im Rahmen der Konzertierten Aktion Mobilität mit Unterstützung der Akademie für Technikwissenschaften (Acatech) einen Datenraum Mobilität für die souveräne und differenzierte Handhabung von Daten als Grundlage moderner Mobilität, auf der Basis von Vertrauen und auf dem Boden europäischer Spielregeln.« (Ebd.: 32)

Und Intermediäre sollen Datenökonomie im Ganzen »souverän« machen, wobei »Souveränität« hier augenscheinlich auch »Dezentralität« (da muss man nachdenken: vielleicht Pluralität der Datenhalter? vielleicht Kundennähe?) meinen kann: »Einen wichtigen Beitrag zur Sicherung des Datenzugangs und -austauschs und zur Stärkung einer souveränen, dezentralen Datenökonomie können vertrauenswürdige Intermediäre leisten.« (Ebd.: 34)

Auch die frühe Bedeutung von »digital souverän« als einer Kompetenz kehrt in abgewandelter Form wieder, sofern durch Bürgerinnen und Bürger, die »souverän mit ihren eigenen Daten umgehen« können, »Datenkompetenz« in allen ihren Facetten souverän ausgeübt werden soll:

»Datenkompetenz verstehen wir im engeren Sinne als die Fähigkeit, individuell und in Organisationen souverän und reflektiert Daten zu sammeln, zu managen, auszuwerten und zu nutzen sowie sich an der gesellschaftlichen Diskussion über den Umgang mit Daten zu beteiligen.« (Ebd.: 41)

»[I]nformiertes und souveränes Handeln der Bürgerinnen und Bürger aller Altersgruppen im Umgang mit Daten« (ebd.: 42) will man unterstützen, zur Intensivierung der Nutzung von Open Source-Software in der Verwaltung erwägt man seitens des Innenministeriums, ein »Zentrum digitale Souveränität« zu gründen (vgl. ebd.: 51), und während das Bundesfamilienministerium ein Projekt »Digitale Souveränität älterer Menschen mit KI-Technologie fördern!« unter seinen laufenden Vorhaben listet, beherbergt das Bundesjustizministerium unter seinem Dach ein Projekt »Datensouveränität und Empowerment von Verbraucher:innen – Datenschutz mit Sprachassistenten« (vgl. ebd.: 88 und 82).

Besonders exquisit sind die Begriffsdefinitionen, die in diesem Durcheinander das Glossar der Datenstrategie für die beiden Begriffe »Datensouveränität« sowie »digitale Souveränität« vorhält:

»Der Begriff *Datensouveränität* geht über das Datenschutzrecht hinaus und stellt die Autonomie der betroffenen Person, aber auch des Unternehmens über ihre bzw. seine Daten in den Mittelpunkt, welche bzw. welcher souverän und durch technische Mittel und seine Fähigkeiten selbstständig in der Lage ist, sich selbstbestimmt in der Datenwelt zu bewegen.« (Ebd.: 110)

»*Digitale Souveränität* beschreibt die Fähigkeit sowohl von Individuen als auch der Gesellschaft, die digitale Transformation – mit Blick auf Hardware, Software, Services, sowie Kompetenzen – selbstbestimmt zu gestalten. Digital souverän zu sein bedeutet im Rahmen des geltenden Rechtes, souverän zu entscheiden, in welchen Bereichen Unabhängigkeit erwünscht oder notwendig ist.« (Ebd.: 111)

Lässt die erste Definition immerhin den Bezug zu einem (zu erweiternden) Datenschutzrecht erkennen, bezieht die zweite die »digitale Souveränität« erst auf das »Individuum«, dann auf »die Gesellschaft« – und dabei auf Technikgestaltung, um schließlich noch die Entscheidung über »erwünschte oder notwendige« Unabhängigkeit als allgemeines Merkmal des Begriffs (wohl: auf allen Anwendungsebenen) nachzuschieben. Vor allem aber sind die Definitionen sowohl zirkulär als auch im Grunde auswechselbar: Einmal geht es um *Autonomie* »über« Daten, *weil* »durch *technische Mittel« sowie »Fähigkeiten« selbständig in der Lage, sich selbstbestimmt zu bewegen* – und das andere Mal um die *Fähigkeit*, digitale Transformation *selbstbestimmt zu gestalten* sowie im geltenden Rechtsrahmen *souverän über Unabhängigkeit* (also erneut so etwas wie Autonomie) *zu entscheiden*.

Von den syntaktischen Schwächen dieser Sätze abgesehen: Wer länger über die beiden Begriffsbestimmungen nachdenkt, den lassen sie nicht nur verwirrt zurück. Vielmehr wird man auch nachdenklich bezüglich des Drucks hinter dieser – ganz offensichtlich ja gut und positiv gemeinten – Versprechungssemantik. Digitaldemokratische Hoffnungen scheint der Souveränitätsbegriff wie ein Traumfänger auf sich zu ziehen und an sich zu binden. Aber dabei verheddern sie sich auch.

## 5. Alles »ein« neues Konzept?

Ab 2019 – von der Leyen hat gesprochen und die Rede der Bundeskanzlerin zur Deutschen EU-Ratspräsidentschaft ist quasi schon in Vorbereitung – setzt die Rezeption vor allem der »digitalen Souveränität« als mögliches neues Leitbild sowohl international als auch in der in Deutschland publizierenden Politikwissenschaft ein. Das Signal aus Brüssel, man wolle einen europäischen Weg der Digitalisierung – der sich nach dem weltweit beachteten Signal der europäischen Datenschutzgrundverordnung tatsächlich auch weiter in Gesetzesvorhaben wie dem *Data Governance Act*, dem *Data Services Act*, dem *Digital Markets Act* und einer eigenständigen, risikobasierten KI-Regulierung abzeichnet – stimuliert die Debatten.

Naturgemäß ist die Wahrnehmung des Stichworts »digital sovereignty« nun eine, die sofort die Bühne der internationalen Politik und auch das Reich der netzethischen und netzpolitischen Szenarien für eine sich rapide weiterentwickelnde Digitalgesellschaft zum hauptsächlichen Kontext macht. Die politische Ideengeschichte der Souveränität kann hierbei – anders als in den oben geschilderten politischen Gebrauchspapieren – mit voller Wucht zum Tragen kommen, auch wenn dies aus Sicht der politischen Philosophie nicht immer auf der Basis profunder Lektüren geschieht. So ruft der Digitalethiker Luciano Floridi 2020 dazu auf, im Digitalzeitalter »the nature of sovereignty« gänzlich neu zu überdenken, denn

> »in the digital age, the infosphere is not a territory, data are not a finite, scarce, rivalrous, natural, non-renewable resource like oil (so much the worse for the poor analogy), digital assets are largely private and subject to market forces, and our profiles are created, owned, and exploited not just by states but also by multinationals, which, as the word indicates, are globalised«. (Floridi 2020: 372)

Die den Staat nun herausfordernden Akteure seien nicht andere Staaten, sondern die großen Digitalkonzerne. Auch politische Macht verändere in diesem Zusammenhang ihre Qualität, es gehe um »Kontrolle«. Aktuelle Streitigkeiten, etwa darum, dass europäische Corona-Apps von Apple und Google abhängig seien, ob das chinesische Huawei in Bieterverfahren für europäische 5G-Technologie einbezogen wird, oder auch die Urteile des EuGH zu den Datentransfer-Abkommen mit den USA, zeigten diesen auf Kontrolle abzielenden Machtkampf an:

> »[T]hese are all episodes in the fight for *digital sovereignty*, that is, for the *control* of *data, software* (e.g. AI), *standards* and *protocols* (e.g. 5G, domain names), *processes* (e.g. cloud com-

puting), *hardware* (e.g. mobile phones), *services* (e.g. social media, e-commerce), and *infrastructures* (e.g. cables, satellites, smart cities), in short, for the *control of the digital*. Let me clarify that by ›control‹ I mean here the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence.« (Floridi 2020: 370 f.)

»Kontrolle«, so Floridi weiter, sei eine graduelle Sache – was dann für eine Art großen Bogen der Machtausübung nicht nur auf staatlicher Ebene, sondern eben auch bis hin zum Individuum sorgt: »[T]he ultimate form of control is *individual sovereignty*, understood as self-ownership, especially over one's own body, choices, and data.« (Floridi 2020: 371)[7] Der Kampf (fight) um digitale Souveränität, so heißt es weiter, sei ein »epochaler«.[8]

Floridi nutzt dieses Lagebild für einen Appell, Europa solle der Gefahr eines »digital sovereignism and statism« begegnen, die drohe, wo man auf einer nationalen digitalen Souveränität beharre: »[T]he best answer to the multinationals' control of the digital is probably the establishment of a (de jure and not only a possibly de facto) supranational digital sovereignty, at the EU level.« (Floridi 2020: 375)

Gehören würden dazu: »digital data sovereignty«, »AI sovereignty«, »5G sovereignty« etc. (als Analogien hierfür gelten interessanterweise die klassischen Hoheitsfunktionen des Staates: »tax sovereignty« und »monetary sovereignty«).

Wie schon zuvor bei der an Deleuze erinnernden Akzentuierung von »Kontrolle« versucht sich Floridi in Anlehnung an moderne philosophische Klassiker (Serres, Foucault) sogar an einem relationalen Konzept der Souveränität:

»One way forward is to recall that sovereignty is not like a rivalrous resource that, when given to someone, is no longer in one's possession, and can only be reacquired by taking it back from that someone. It is more like a relation (control), in which one may engage

7 Unschwer zu erkennen beerbt Floridi hier in vager Form zum einen die einem wirkungsreichen Essay des Philosophen Gilles Deleuze entlehnte Vorstellung, Digitalgesellschaften seien »Kontrollgesellschaften«, zum anderen eine an Michel Foucault orientierte Idee von mikrologischen Machtprozessen, die das Individuum formen. Vor allem Deleuzes knappe Überlegungen zur Kontrolle sind in den Digitaldebatten der vergangenen zwei Jahrzehnte zur Vulgärmetapher geronnen. Auch Floridis schlichte Definition von Kontrolle als Möglichkeit der Einflussnahme hat jedenfalls mit Deleuze und Foucault wenig zu tun.

8 »… epochal struggle not only for all against all, but also of anyone allied with anyone, with variable alliances changing according to interests and opportunities« (Floridi 2020: 371).

more or less intensely and successfully, but precisely because it is a matter of engagement is never ›lost‹ when exercised or delegated, and is not finite or rivalrous: giving it to someone does not mean being unable to give it also to someone else at the same time. Such a relational concept of sovereignty enables one to see that the legitimisation of sovereignty can be modelled in terms of the topology of the network that seems to be the most appropriate for its structuring.« (Floridi 2020: 376)

Ein solches Netzwerk solle keine vollvernetzte, verteilte und auch keine zentralistisch-sternförmige, sondern eine hybride Topologie haben, in welcher sich Knoten hierarchisch unterschiedlich legitimieren. Die Eurozone dient als Beleg: Auch Staaten seien heute »individual multiagent systems«.

»This is how the ›combined sovereignty‹ of the EU may be understood and promoted. Through the mechanism of ›enhanced cooperation‹, a hybrid network could support a core of more federal Europe within a larger, more confederated EU, and call the whole the United States of Europe. [...] Not an easy thing to do, but, if I am correct, one day the United States of Europe will not be an intergovernmental or supranational chapter in the history of the Westphalian state and its analogue/digital sovereignties, but a new book altogether, neither a confederation nor a federation, but a differentiated integration with its own design.« (Floridi 2020: 377)

Mit einer Perspektive wie dieser wird der »europäische Weg« der Datenpolitik nicht nur befürwortet, sondern mit politisch-theoretischem Vokabular aufgeladen und zur Systemkonkurrenz historischen Ausmaßes hochstilisiert. Zugleich schießen Belange der Mikroebene und die nationale oder aber transnationale Makro-Ebene irgendwie zusammen: die digitale Souveränität wäre demnach eine Art Leitbild für den Weg in eine neue Form von »digitaler« Demokratie der Zukunft. Nicht ganz unähnlich suggeriert auch die Rede zur Kandidatur der Kommissionspräsidentin von der Leyen, technologisch souverän zu sein schließe Individualgrundrechte (»Werte«) in nicht näher explizierter Weise, aber jedenfalls rechtsstaatlich erwünschter Weise mit ein.

Parallel zu solchen programmatischen Perspektiven greifen auch deutlich skeptischere Kommentatorinnen und Kommentatoren die »digitale Souveränität« als ein umfassendes Leitbild auf. Für sie meldet sich in Gestalt des neuen Programmworts gleichsam »der« Staat – wenn nicht sogar: ein »starker« Staat – in einer zeitweilig eher staatsfern wirkenden Debatte neu zu Wort, und zwar um Machtansprüche zu stellen. So mahnt die Kulturwissenschaftlerin Julia Pohle für Europa, aber auch für die deutschsprachige öffentliche Diskussion an, man solle, statt auf digitale Souveränität zu pochen, die »demokratische Selbstbestimmungsfähigkeit der Bürgerinnen

und Bürger in ihrer Gesamtheit« in den Vordergrund rücken, und zudem müsse eine »Abgrenzung zum Souveränitätsdiskurs autoritärer Staaten« stattfinden (vgl. Pohle 2020b: 21). Schon 2019 haben Pohle und Thorsten Thiel eine Studie zum Konzept »digitale Souveränität« vorgelegt. Mit dem US-amerikanischen Informations-Ökonomen Milton Mueller, der zu den politischen Konzepten der entstehenden Netzgesellschaft forscht, rücken sie die aktuelle europäische Souveränitäts-Semantik in den Zusammenhang des emanzipatorischen Ringens der Cyberpioniere der 1990er und 2000er Jahre darum, sich abzulösen von politischer Staatlichkeit herkömmlichen Typs, um den digitalen Raum zu einer deterritorialen, hierarchiefreien oder jedenfalls in ihren – auf liberale Kollektive setzenden, vielfach technikgestützten – Partizipationsmustern autonomen Gegengesellschaft auszubauen (vgl. Pohle/Thiel 2019a). Bekanntlich haben sich derartige netzpolitische Programme unter anderem mit spektakulären Manifesten bekannt gemacht. »You are not welcome among us. You have no sovereignty where we gather«, schleudert John Perry Barlows *Unabhängigkeitserklärung des Cyberspace* den »Governments of the Industrial World«, »weary giants of flesh and steel« entgegen, und kündigt unter anderem an:

> »In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.« (Barlow 1996)

Pohle und Thiel zeichnen nach, wie nicht nur der utopische, sich von der »physischen« Wirklichkeit abwendende Cyber-Aktivismus, sondern auch der nachfolgende quasi reformistische, nämlich auf eine freiheitliche Transformation politischer Strukturen vom Netz her setzende »Internet-Governance-Diskurs« die Idee einer »souveränen« Selbstorganisation wenn nicht aufgeben, so doch mindestens stark relativieren muss. Nationalstaaten behalten nicht nur faktisch Zugriffsmöglichkeiten auf essenzielle Elemente des Netzes, sondern besitzen auch die Fähigkeit und den Willen, digitalpolitisch im Eigeninteresse aktiv zu sein, ja das Netz zum Werkzeug forcierter Nationalismen zu machen. Den Autoren zufolge könne »digitale Souveränität« als Losung im Dienst genau solcher staatlichen Bestrebungen verstanden werden. Namentlich China, aber auch Russland legen sie offensiv an den Tag. Freilich habe auch derjenige Debattenstrang, der Souveränität weniger als Abgrenzung nach außen denn als Sache von Partizipation und informationeller Selbstbestimmung proklamiere, einen

»stark präskriptiv-normativen« Charakter, es gehe um das »Wieder-Einsetzen von Souveränität im Namen von Demokratie und Selbstbestimmung« (Pohle/Thiel 2019a: 13 sowie 2019b: 71).

»Dass der Begriff« – nämlich »digitale Souveränität« – »von staatlichen Akteur*innen propagiert wird, ist wenig überraschend. Aber dass er auch offensiv von Wirtschaft und Zivilgesellschaft umarmt wird, sollte schon etwas mehr stutzig machen«, warnen die Autoren (vgl. Pohle/Thiel 2021: 320) in einem Beitrag, der diese Analyse fortschreibt. Sie sprechen nun von einem »einenden, aber problematischen Konzept«, das zwar in Deutschland stärker als anderswo »in den Kontext individueller Selbstbestimmung gerückt« werde:

»Statt allein die Unabhängigkeit und Autorität des Staates im Digitalen zu betonen, gilt im deutschen Diskurs also digitale Souveränität als Voraussetzung dafür, den Prozess der digitalen Transformation mitzugestalten und im digitalen Raum selbstbestimmt handeln zu können. Und dies bezieht sich gleichermaßen auf den Staat als zentralen demokratischen Akteur wie auch auf die Bürger*innen als individuelle Nutzer*innen und Konsument*innen.« (Pohle/Thiel 2021: 329 f.)

Dennoch: »Die Prominenz des Begriffes macht ihn zu einer starken normativen Projektionsfläche.« (Pohle/Thiel 2021: 337) Man grenze sich mit dieser Akzentsetzung »unter dem Vorwand einer europäischen Sozial- und Verbraucherpolitik« (Pohle/Thiel 2021: 337) von Staaten wie China ab. Auch die oft verwendete Doppelforderung nach digitaler Souveränität für Deutschland »und« Europa sehen die Autoren kritisch: »Das Verwischen der Grenze zwischen Nationalstaat und Europa – wie es in deutschen Positionspapieren anhaltend praktiziert wird – lässt sich durchaus als Interessenpolitik einer ohnehin sehr dominanten Macht wahrnehmen.« (Pohle/Thiel 2021: 338) Digitale Souveränität wäre demnach ein Stück Rückeroberung nationalstaatlicher Hegemonie, wenngleich im deutschen und europäischen Sprachspiel in einem – aber möglicherweise trügerischen – demokratischen Gewand. Als Beleg unterziehen die Autoren einen FAZ-Artikel des Informatikers Christoph Meinel, *Deutschland gibt seine Souveränität am Router ab* (Meinel 2020), einer ideologiekritischen Lektüre: Erst einmal vertrete Meinels Text zwar einen »progressiven Souveränitätsbegriff« (Pohle/Thiel 2021: 338), dann aber – und zwar

»wo der Text aber explizit auf die politische Ebene eingeht, ändert sich plötzlich der Ton und eine andere Vorstellung von Souveränität und ihrer Funktion wird deutlich. Meinel problematisiert […] demokratische Prozesse und Institutionen und beschreibt diese als

eher hinderlich für das technische Konzept digitaler Souveränität. Hier zeigt sich exemplarisch, dass der Souveränitätsbegriff – gerade weil er so diffus und doch zielgerichtet verwendet wird – oft viel zu sehr vom als wünschenswert unterstellten Ergebnis her gedacht ist und weniger als ein demokratischer Prozess.« (Ebd.: 339)

Noch pointierter geht Thorsten Thiel, ebenfalls in einem FAZ-Essay, *Das Problem mit der digitalen Souveränität*, mit dem aus seiner Sicht ideologischen Begriff ins Gericht. Die Forderung nach digitaler Souveränität, die in Europa während der deutschen EU-Ratspräsidentschaft »an Intensität gewonnen« habe, sei, so Thiel, zu deuten als Anzeichen eines »neuen geopolitischen Bewusstseins«, eines irregeleiteten Kontrollwunschs westlicher Demokratien sowie als öffentlicher (oder vielleicht auch politisch-administrativer) »Abwehrreflex«, welcher »eine demokratische Selbstverständigung auf das Moment der Selbstbehauptung verkürzt« (Thiel 2021). Letztlich leiste die Forderung nach digitaler Souveränität ungewollt neuen Durchgriffs- und Kontrollmechanismen Vorschub und drohe in Europa und auch Deutschland mit Freiheitsrechten in Widerspruch zu geraten.

## 6. Konzeptionelle Wegweiser?

Beobachten wir auf der einen Seite also – Beispiel Datenstrategie der Bundesregierung von 2021 – eine besorgniserregende, geradezu babylonische Vervielfältigung und Vermischung der Termini, so sehen wir auf der anderen Seite – Beispiel EU-Politik, Beispiel aber auch Pohle und Thiel – wie ein und dieselbe Vokabel gleichsam anschwillt: die Diskurslage wird zusammengebacken und verschmolzen zu einem einzigen ideologischen Souveränitäts-Syndrom. Während im einen Fall die Differenz von Daten- und digitaler Souveränität gesucht wird (wenn auch nicht immer gefunden), wird sie im anderen Fall überhaupt nicht wirklich registriert. Pohle und Thiel deuten Komposita wie »Daten-« oder »Verbrauchersouveränität« (wie auch von der Leyens »technologische« Souveränität) lediglich als typisch deutsche Weiterungen einer alles dominierenden »digitalen« Souveränität im zwischenstaatlich-völkerrechtlichen Sinn. Auch entgeht ihnen, dass im Kontext von Daten- wie von digitaler Souveränität gerade die Datenstrategie der Bundesregierung einen Kompetenz-Ansatz verfolgt, welcher das Ziel des »souverän«-Werdens geradezu rührend eng an didaktische Vorstellungen einer Befähigung des Einzelnen knüpft. Digitale Transformation selbstbestimmt gestalten zu wol-

len: dieser generelle Wunsch lässt sich bei bestem Willen nicht in plausibler Weise als per se bereits ein Vehikel der Re-Nationalisierung entlarven, und auch nicht als Gedanke, der – wie der »digitalen Souveränität« zur Last gelegt – »Zentralisierung und Machtdurchsetzung prämiert« (vgl. Pohle/Thiel 2021: 340). Zweifel sind überdies nicht nur dort angebracht, wo keinerlei begriffsgeschichtliches Interesse zu verspüren ist – wo die Bundesregierung »Datensouveränität« sagt, ignoriert sie die frühe, bloße Skills meinende Bedeutung des Ausdrucks ebenso wie die (allerdings in Deutschland generell kaum rezipierte) internationale Debatte über »indigenous data sovereignty« (Kukutai/Tayler 2016). Zweifeln macht vielmehr auch die Reduktion der Genealogie des Souveränitätsbegriffs auf die kurze Spanne der netzpolitischen Auseinandersetzungen um ein »souveränes« Internet. Wenn Pohle und Thiel der Versuchung erliegen, die Verlautbarungen der europäischen Politik in diese Tradition zu stellen, lehnen sie sich womöglich doch zu einseitig an eine auf die US-amerikanischen Cyberbewegung und Medientheorie verengte und letztlich akademisch-ideologiekritische Sichtweise an.

Netzpolitische Debatten und breit öffentliche Resonanzräume auf dem Kontinent sind zweierlei. Deutlich wahrscheinlicher ist es, dass die deutsche und europäische Öffentlichkeit, wenn die Rede von Datensouveränität, was ja tatsächlich der Fall ist, wie ein Lauffeuer funktioniert, an demokratische Partizipation und politische Mitgestaltungsansprüche denkt. Vielleicht sogar an Volkssouveränität. Wo der Ruf nach Datensouveränität oder digitaler Souveränität ertönt, wird man sich weniger darum reißen, ist in einer Konkurrenz der Nationalstaaten wahrzunehmen, als darum, den digitalen Wandel nicht mehr aus einer Position reiner Ohnmacht erleben zu müssen. Auch die Assoziation »Zentralismus« erscheint – gerade was die Digitalpolitik angeht – weder für die digitalpolitisch und was den Datenschutz angeht föderale Bundesrepublik noch für das aus Sicht seiner Bürgerinnen und Bürger vorwiegend durch Fliehkräfte geprägte, notorisch prekäre Europa passend.

Eher schon steckt im Ruf nach mehr Souveränität eine Art Notstandslogik. Haben die Regierungen mit ihren klassischen Mitteln der Gesetzgebung und der Rechtsdurchsetzung überhaupt noch das Heft des Handelns in der Hand? Oder sollten, wo so wenig Staat herrscht, wie in digitalen Räumen, nun nicht wenigsten die Nutzer zur Notwehr berechtigt werden und endlich auf eigene Faust für Ordnung sorgen können?

In der Tat erleben Bürgerinnen und Bürger ja durchaus Abhängigkeiten und Ohnmacht im Zusammenhang mit Digitalisierung. Viele erleben eben nicht nur Fortschritt, immer schnellere und bessere digitale Vermitt-

lungen, sondern auch eine befremdliche Sozialität in Netzwelten, ein Leerlaufen des geltenden Rechts, einen zu schwachen Schutz kritischer Infrastrukturen und eine Ohnmacht von Kartell- und Strafverfolgungsbehörden erleben. Wer sich im Netz als Freiwild fühlt, will nicht, wo der Staat eingreift, erneut eher die inländischen Nutzerinnen und Nutzer reglementiert sehen als Trolle und Netzgiganten. Hierauf reagieren auch die Subjekte eines im Kleinen überakribisch, im Großen nachlässig wirkenden Datenschutzes, der sich auf das »Klick« des immer wieder neuen Zustimmens beschränkt. Letztlich erwarten Bürgerinnen und Bürger keinen starken Staat, aber einen Primat der Politik, und zwar einer Politik, die sie selbst auch wirklich mandatieren und legitimieren können. Diesen Tenor scheinen auch Stimmen von der europäischen Bühne zu haben, wenn sie aktuell bilanzieren:

»There is growing concern that the citizens, businesses and Member States of the European Union (EU) are gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment. Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field.« (EPRS 2021: 1)

Zugespitzt gesagt, steckt insofern hinter dem Ruf nach »Souveränität« nicht eine wiedererstarkende Nationenkonkurrenz, sondern die Forderung nach mehr digitaler *citoyenneté*.

Einig sind sich die Autoren immerhin in der Klage über die uneinheitliche Begriffsverwendung – und dies insbesondere zum Nachteil der »Datensouveränität«. Denn leider ist die mit *diesem* Begriff verbundene, den Status der informationellen Selbstbestimmung betreffende deutschsprachige Debatte noch gar nicht geführt, scheint jetzt aber durch die »digitale« Souveränität (wie auch die vielen anderen Souveränitäten) überlagert zu werden.

»Wir verwenden den Begriff pragmatisch-konstruktiv« (Hummel u. a. 2021a: VII), hat unlängst ein Autorenteam in Sachen Datensouveränität vorgeschlagen. Mir scheint, vor allem tut man zunächst gut daran, für die Zwecke einer deutschsprachigen Diskussion, die auch seitens der Bürgerinnen und Bürger geführt werden soll, die nun einmal deutlich unterschiedene konzeptionelle Genese von »Datensouveränität« einerseits und »digitaler Souveränität« andererseits zu beherzigen – und darauf zu beharren, dass beides möglichst erst einmal zweierlei bleibt. Weder ist die zwischenstaatliche Dimension und die Frage des regierungsseitigen Umgangs mit inter- und transnationalen Abhängigkeiten ausdiskutiert, noch sollte man die mit Impulsen in Sachen Datensouveränität begonnenen Diskussionen

abbrechen lassen, die auf die Weiterentwicklung eines Datenschutzes dringen, welcher womöglich der demokratischen *agency* von Bürgerinnen und Bürgern nicht (mehr) entspricht.

»Souveränität« wiederum muss man als Terminus weder verteufeln noch hat, wer ihn verwendet, automatisch zentralstaatlich argumentiert, Hobbes oder gar Carl Schmitt fetischisiert. Nach dem Wo, dem Wann und vor allem dem Wie politischer Souveränität zu fragen, gehört vielmehr zu den elementaren demokratischen Mechanismen – und ist gerade im unübersichtlichen Feld der Technologiepolitik eigentlich sogar permanent geboten. Hinzu kommen legitime Zweifel an der Durchsetzungskraft des Rechtsstaates, wo man »Schutz« verspricht, dieser vielfach offenkundig aber leerläuft. Wenn man den Eindruck hat, dass Digitalisierung gleichsam Schicksal wird und unterschwellig mit so etwas wie Staatsversagen einhergeht, weil eine demokratische *agency* nicht mehr vorgesehen ist, dann spätestens merkt jede und jeder, dass Schutz – jedenfalls bloßer Schutz – eben gerade keine Selbstbestimmung ist.

# Konsumentensouveränität und Datensouveränität aus ökonomischer Sicht

*Wolfgang Kerber und Karsten K. Zolna*

## 1. Einleitung

Eine der zentralen Fragen der digitalen Transformation von Wirtschaft und Gesellschaft besteht darin, ob und inwieweit Individuen in der Lage sind oder sein sollten, über den Zugang zu und die Verwendung von »ihren« Daten zu entscheiden. Diese scheinbar simple Frage ist äußerst komplex mit vielfältigen Dimensionen. Assoziiert man in einer vordergründigen Weise diese Frage mit dem Begriff der »Datensouveränität«, so könnte eine Interpretation dieses Begriffes darin bestehen, dass Individuen »souverän« darüber entscheiden können (sollen), wer Zugang zu »ihren« Daten bekommt, das heißt wer sie beispielsweise sammeln darf, und wie diese Daten verwendet werden (sollen). Die Fragen sind hier bewusst doppelt gestellt, nämlich zum einen im Hinblick auf eine positive Aussage (das heißt, ob und inwieweit die Individuen tatsächlich souverän über »ihre« Daten entscheiden können), und zum anderen im Hinblick auf eine normative Aussage, nämlich ob und inwieweit sie das Recht haben sollten, souverän über »ihre« Daten zu entscheiden. Die hier bei »ihren« Daten verwendeten Anführungszeichen machen zugleich deutlich, dass zu dieser Frage auch das Problem gehört, welche Daten zu dieser Menge »ihrer« Daten gehören sollen. Wir werden uns in diesem Beitrag vor allem auf die datenschutzrechtlichen Einwilligungen der Individuen in Bezug auf ihre personenbezogenen Daten konzentrieren. Aktueller Hintergrund ist die weltweit stattfindende Diskussion über das Problem, dass die Menschen in einer sich digitalisierenden Welt zunehmend die Kontrolle darüber verlieren, wer welche Daten über sie sammelt und wie diese verwendet werden. Hieraus resultieren für die Menschen vielfältige Risiken, beispielsweise für ihre Privatsphäre und (Cyber-)Sicherheit, aber auch für ihre Entscheidungsautonomie über die Frage, wie diese Daten

genutzt werden sollen. Hieraus können dann Forderungen nach einer Stärkung der »Datensouveränität« abgeleitet werden.

Unser Beitrag hat das Ziel zu zeigen, wie diese Fragen aus einer ökonomischen (und damit auch wirtschaftspolitischen) Perspektive adressiert werden können. In der ökonomischen Diskussion über Daten wird der Begriff der »Datensouveränität« nicht verwendet. Dies hat sicherlich seinen Grund auch darin, dass der (stark staatsrechtlich geprägte) Begriff der »Souveränität« nur in sehr begrenztem Umfang in der Ökonomie benutzt wird. Faktisch spielt er nur im Rahmen der Verwendung des Begriffs »Konsumentensouveränität« (»consumer sovereignty«) eine zentrale Rolle, insbesondere im Rahmen der ökonomischen Analyse von Verbraucherverhalten und damit auch der Verbraucherpolitik (als einer speziellen Wirtschaftspolitik). Diese hat gerade auch die Aufgabe, die Konsumentensouveränität der Verbraucherinnen und Verbraucher zu stärken, damit diese durch ihre Konsumentscheidungen besser ihre Konsumentenpräferenzen erfüllen können.

Da Entscheidungen über die datenschutzrechtliche Einwilligung zur Sammlung und Nutzung von personenbezogenen Daten eine sehr zentrale Rolle bei Konsumentscheidungen in der digitalen Welt spielen, beispielsweise als Bezahlung für vielfältige (monetär) unentgeltliche digitale Dienstleistungen, ist es naheliegend, die Frage nach der »Datensouveränität« von Individuen aus der ökonomischen Perspektive dieses wohletablierten Ansatzes der Konsumentensouveränität und auch der Verbraucherpolitik zu analysieren.[1] Die datenschutzrechtliche Einwilligung nach Art. 6 (1)a DSGVO in vertragliche Vereinbarungen, welche festlegt, wer welche personenbezogenen Daten sammeln und für welche Zwecke nutzen darf, kann damit als Teil einer solchen »souveränen« Entscheidung von Konsumenten verstanden werden. Insofern ist es aus ökonomischer Sicht auch nicht überraschend, dass das Datenschutzrecht, das die Rechte der Datensubjekte über die Nutzung personenbezogener Daten regelt, auch als eine spezielle Form der Verbraucherpolitik bezeichnet werden kann.[2] Hierbei muss immer mitbedacht werden, dass das datenschutzrechtliche Instrument der Einwilligung auch ein zentrales Instrument der Konsumenten ist, um ihre Privatsphäre zu schützen, beispielsweise auch in Bezug auf die

1 Vgl. zu den vielfältigen und auch verwirrenden Arten der Verwendung des Begriffs »Datensouveränität" Hummel u. a. 2021b sowie den Beitrag von Gehring in diesem Band.

2 Vgl. aus juristischer Sicht Graef u. a. 2018 und aus ökonomischer Perspektive Kerber 2016: 642 ff.

vielfältigen Risiken, die kurz- oder längerfristig mit der Weitergabe von personenbezogenen Daten verknüpft sein können.[3]

Der Beitrag ist folgendermaßen strukturiert. Im nächsten kurzen Abschnitt 2 wird zunächst auf die Entwicklung des Begriffs der Konsumentensouveränität in der Ökonomie eingegangen. In Abschnitt 3 wird ein knapper Überblick über die Rolle des Konzepts der Konsumentensouveränität in der ökonomischen Verbraucherpolitik und über zentrale verbraucherpolitische Instrumente gegeben, insbesondere im Hinblick auf die Stärkung der Konsumentensouveränität. Im Hauptteil des Beitrags (Abschnitt 4) wird dieser Ansatz dann auf die Probleme von Entscheidungen von Konsumenten in Bezug auf ihre Daten in der digitalen Ökonomie angewendet. Hierbei wird sich zeigen, (a) dass ihre »Datensouveränität« durch verschiedene Marktversagensprobleme, insbesondere durch Informationsasymmetrien und (verhaltenswissenschaftlich begründete) Rationalitätsprobleme, stark eingeschränkt ist, (b) welche Diskussionen über wirtschaftspolitische bzw. rechtliche Lösungen zur Stärkung der »Datensouveränität« der Konsumenten geführt werden, und (c) welche Probleme und Grenzen hierbei auftreten. Abschließend werden in Abschnitt 5 noch kurz weitergehende, wichtige Fragen in Bezug auf die »Souveränität« von Individuen über »ihre« Daten aufgezeigt, die hier in diesem Beitrag nicht behandelt werden. Dies bezieht sich auf die Frage, über welche Daten Verbraucher überhaupt individuelle Entscheidungen treffen können (das heißt »souverän« entscheiden) sollen und inwieweit auch andere Akteure Rechte in Bezug auf die Nutzung dieser Daten haben sollen. Aus ökonomischer (aber auch rechtlicher Sicht) ist dies die Frage nach der richtigen Spezifizierung und Zuordnung eines Bündels von Rechten (»bundle of rights«) an Daten.

## 2. Zur Entwicklung des Begriffs »Konsumentensouveränität« in der Ökonomie

Der Begriff der »Souveränität« wird in der Ökonomie üblicherweise nicht direkt verwendet. Allerdings spielen damit verbundene Fragen auch in

3 Solche Risiken können beispielsweise entstehen durch Identitätsmissbrauch, Preisdiskriminierung, betrügerische und manipulative Praktiken und das Erstellen von tiefgehenden Konsumentenprofilen (OECD 2020: 22).

der Ökonomie eine zentrale Rolle – aber unter Verwendung anderer Begrifflichkeiten. Interessanterweise wird nationalstaatliche Souveränität in wirtschaftlicher Sicht, nämlich wirtschaftliche Autarkie, von der Ökonomie seit Adam Smith und David Ricardo negativ bewertet, weil durch sie die Vorteile der internationalen Arbeitsteilung zwischen den nationalen Volkswirtschaften nicht genutzt werden. Hieraus wurde immer die Forderung nach Freihandel und dem Abbau von Hindernissen für die internationale Arbeitsteilung abgeleitet. Die aktuelle Diskussion um Forderungen nach einer größeren »digitalen Souveränität« Deutschlands oder der EU steht folglich in einem prinzipiellen potenziellen Widerspruch zu der in der Ökonomie vorherrschenden Vorstellung einer globalen, auf internationaler Arbeitsteilung basierenden Handels- und Wirtschaftsordnung. Solche Forderungen benötigen deshalb aus ökonomischer Sicht einer sehr sorgfältigen und differenzierten Begründung.[4] Von viel zentralerer Bedeutung ist dagegen die Idee von freien, autonomen Entscheidungen von Individuen und Unternehmen (Privatautonomie), durch die erst marktwirtschaftliche Systeme entstehen können, die ja bekanntlich auf dezentralen Entscheidungen bezüglich des Angebotes und der Nachfrage von Produkten und Dienstleistungen auf Märkten basieren. Dies setzt aus ökonomischer Sicht neben Privateigentum und Vertragsfreiheit nicht nur die unternehmerische Freiheit zur Innovation voraus, sondern vor allem auch die Freiheit der Konsumenten, zwischen verschiedenen Angeboten diejenigen auszuwählen, die am besten ihren Wünschen entsprechen bzw. ihre Probleme lösen. In diesem Sinne ist die Idee »souveräner« Entscheidungen von individuellen Akteuren (Unternehmen, Personen) konstitutiv in der Ökonomie marktwirtschaftlicher Systeme verankert, auch wenn der Begriff individueller »souveräner« Entscheidungen üblicherweise nicht in mikroökonomischen Lehrbüchern zu finden ist.

Die Einführung des spezifischen Begriffs der »Konsumentensouveränität« in die Ökonomie wird üblicherweise William Harold Hutt zugeschrieben (in seinem 1936 erschienenen Buch »Economists and the Public: A Study of Competition and Opinion«).[5] Er verwendet den Begriff, um die »Macht« zu beschreiben, die Konsumenten auf Märkten durch ihre Freiheit haben,

4 Vgl. kritisch zur europäischen Industriepolitik beispielsweise Hefeker 2020.

5 Hutt 1936; vgl. zur folgenden Diskussion in der Ökonomie Fraser 1939, Hutt 1940, Lerner 1972 und Persky 1993.

selbst zwischen verschiedenen Produkten wählen zu können.[6] In dieser Verwendung wird der Konsument gerade nicht als schwach beschrieben, sondern als jemand, der durch seine Konsumentscheidung Macht in Bezug auf den Einsatz von Ressourcen einer Volkswirtschaft direkt ausüben kann. Was damit ausgedrückt wird, ist die bis heute dominierende Vorstellung in der Ökonomie, dass auf wohlfunktionierenden, wettbewerblichen Märkten den Anbietern Anreize gesetzt werden, ihre Produkte und Dienstleistungen an den Wünschen der Konsumenten auszurichten, dass es also die Nachfrage ist, die das Angebot bestimmt. Da man den Wettbewerb als einen Prozess verstehen kann, in dem Anbieter mit ihren Leistungen um die Nachfrager konkurrieren, ist die Macht von Verbrauchern auch damit verknüpft worden, darüber zu entscheiden, wer ihnen die besseren Leistungen anbietet (mit der Folge von steigenden bzw. sinkenden Marktanteilen und Gewinnen der jeweiligen Anbieter).[7] Insofern sind es die Konsumenten, die mit ihren Entscheidungen als Endnachfrager über die Allokation der Ressourcen einer Volkswirtschaft mitbestimmen. Schon früh wurde dies auch mit der Idee einer Analogie zu demokratischen Wahlentscheidungen assoziiert, bei der Verbraucher mit ihren Entscheidungen, wie sie ihr Geld ausgeben, ihre »Stimmzettel« darüber abgeben, welche Produkte sie besser finden.[8] Folglich wurde mit dem Begriff der Konsumentensouveränität die »Macht« verbunden, die Verbraucher auf Märkten als Nachfrager ausüben können.[9] Dies kann sowohl als eine positive Aussage über die Funktion von Konsumenten auf Märkten verstanden werden, aber auch als eine normative Aussage darüber, welche Funktion sie auf Märkten ausüben sollten, damit diese gut funktionieren.

Aus dieser Perspektive ist es nicht überraschend, dass sich dann der Begriff der Konsumentensouveränität aus ökonomischer Sicht mit der seit den 1960er und 1970er Jahren breit entwickelnden Verbraucher(schutz)politik

6 »The consumer is sovereign when, in his role of citizen, he has not delegated to political institutions for authoritarian use the power, which he can exercise socially through his power to demand (or refrain from demanding)« (Hutt 1936: 257).

7 Vgl. zum »Wettbewerb als Entdeckungsverfahren« Hayek 1968.

8 Vgl. Persky 1993: 185, der auf das Buch des Ökonomen Fetter 1905 sowie später Wilhelm Röpke und Friedrich August von Hayek verweist, die bereits in den 1930er Jahren auch diese Analogie verwendet haben. Hierbei ist allerdings auch erkannt worden, dass durch eine ungleiche Einkommens- und Vermögensverteilung die »Stimmen« der Konsumenten sehr ungleich verteilt sein können.

9 Vgl. Persky 1993: 184, der dies in dem Satz zusammenfasst: »Consumer sovereignty gives power to consumers«.

verknüpfen lässt, die umgekehrt gerade thematisiert, dass in der Realität die Verbraucher auf vielen Märkten oft große Probleme haben, diese Rolle faktisch auszufüllen. Während sowohl die Ökonomie als auch das Privatrecht theoretisch von der Fiktion von frei ausgehandelten Verträgen zwischen (auf »Augenhöhe« agierenden) gleichberechtigten Marktpartnern ausgehen, hat sich der Verbraucherschutz mit seinen vielfältigen Ausdifferenzierungen aus der praktischen Erfahrung entwickelt, dass Verbraucher auf vielen Märkten die »schwächere« Marktseite sind (etwa gegenüber großen Unternehmen), weswegen sie eines besonderen Schutzes bedürfen. Die Entwicklung des Verbraucherrechts war deshalb immer das Resultat konkreter Probleme von Verbrauchern auf bestimmten Märkten, die dann mit speziellen verbraucherpolitischen Instrumenten zu lösen versucht wurden. Die Verbraucherpolitik bestand dabei stets aus einer Mischung von Instrumenten, die einerseits auf eine Stärkung der Fähigkeiten von Konsumenten abzielten, selbst für sich gute Entscheidungen zu treffen, und andererseits anderen Instrumenten, die die Gesundheit, Sicherheit und ökonomischen Interessen der Verbraucher direkt schützen sollten. Hierbei werden auch regulatorische Instrumente eingesetzt, die zu einem erheblichen Teil auch als »paternalistisch« interpretiert werden können.[10] Die heute überall in der Verbraucherpolitik im Mittelpunkt stehende Forderung nach »consumer empowerment« kann deshalb direkt damit verbunden werden, dass die Konsumenten besser in die Lage versetzt werden sollen, durch ihre eigenen Entscheidungen auf Märkten ihre Interessen stärker durchzusetzen, und damit auch die mit dem von Hutt geprägten Begriff »Konsumentensouveränität« verbundene Rolle besser auszuüben. Insofern sind es die real bestehenden Defizite der Konsumentensouveränität, die die Verbraucherpolitik mit ihren Instrumenten adressieren möchte.[11] Im folgenden Abschnitt 3 werden wir genauer aus ökonomischer Sicht analysieren, welche Probleme hierbei typischerweise auftreten und mit welchen Instrumenten die Verbraucherpolitik diese Probleme zu lösen versucht, bevor wir dann in Abschnitt 4 auf die spezifischen Probleme von Konsumenten mit ihren Entscheidungen über Daten in der digitalen Ökonomie eingehen.

10 Vgl. zu dieser Problematik aus einer rechtswissenschaftlichen Perspektive Drexl 1998: 282 ff. und 449 ff.

11 Vgl. zur Verbraucherpolitik aus ökonomischer Sicht generell OECD 2010, Luth 2010, Siciliani u. a. 2019.

## 3. Konsumentensouveränität und Verbraucherpolitik

Der Verbraucherschutz mit der Vorstellung von »schwachen« (oder in heutiger Diktion »vulnerablen«) Konsumenten, die in gewissem Umfang speziell geschützt werden müssen,[12] hat sich im Recht Schritt für Schritt entwickelt. Wie hat die Ökonomie versucht, dieses Problem mit ihrem theoretischen Instrumentarium zu fassen? Zentraler normativer Bezugspunkt in der Ökonomie ist das Modell der vollkommenen Konkurrenz (»perfect competition«), in dem Wettbewerb herrscht und alle Marktbeteiligten rational handeln und vollständig informiert sind. Ökonomen war immer bewusst, dass die weitgehenden Bedingungen dieses Modells auf realen Märkten fast immer nur in beschränktem Umfang erfüllt sind, das heißt dass es fast immer mehr oder minder große Abweichungen von diesem Idealmodell gibt (»Marktunvollkommenheiten«). Basierend auf dieser Erkenntnis hat die Ökonomie eine Anzahl unterschiedlicher Marktversagensarten definiert sowie daraus folgende spezielle Wirtschaftspolitiken zur Lösung dieser spezifischen Marktversagensprobleme entwickelt.[13] Allerdings sind nur ein Teil der Marktversagensarten für die Verbraucherpolitik relevant. Obwohl beispielsweise fehlender Wettbewerb durch marktmächtige Unternehmen oder Kartelle sich zweifellos (beispielsweise durch höhere Preise) negativ auf Konsumenten auswirkt, war dieses Problem nie Teil der Aufgaben der Verbraucherpolitik, sondern der Wettbewerbspolitik, die durch den Schutz des Wettbewerbs indirekt auch die Verbraucher schützen soll. Aus ökonomischer Sicht sind es zwei andere Marktversagensarten, die zu der in der Verbraucherpolitik thematisierten »Schwäche« der Verbraucher führen: Dies sind einerseits Informationsprobleme der Konsumenten, das heißt dass sie nicht so gut informiert sind, wie im idealen ökonomischen Marktmodell unterstellt, und zum anderen Rationalitätsprobleme, das heißt, dass wir als Verbraucher unter bestimmten Umständen nicht immer so rational handeln, wie es das ökonomische Bild des Menschen als Homo oeconomicus unterstellt, das im Modell des vollkommenen Wettbewerbs verwendet wird. Eine solche auf diese beiden Marktversagensarten abstellende Konzeption

---

12 Hierbei ist zu berücksichtigen, dass die Verbraucherpolitik auch schon lange miteinbezieht, dass verschiedene Gruppen von Konsumenten in unterschiedlichem Umfang »vulnerabel« sein können.

13 Vgl. zur ökonomischen Marktversagenstheorie und den daraus sich ergebenden Wirtschaftspolitiken das Lehrbuch von Fritsch [18]2018.

der Verbraucherpolitik hat sich inzwischen in der verbraucherpolitischen Diskussion breit durchgesetzt.[14]

Diese beiden Marktversagensarten können wie folgt näher erläutert werden:

(1) Für die Analyse von Informationsproblemen der Konsumenten kann auf die Informationsökonomie zurückgegriffen werden.[15] Da die Informationssuche meist Kosten verursacht, ist es rational, sich nur beschränkt zu informieren, sodass Konsumentscheidungen unter unvollkommener Information getroffen werden. Mindestens ebenso bedeutsam sind aber die vielfältigen Probleme, die auf Informationsasymmetrien zwischen Anbietern und Konsumenten beruhen. Diese können dazu führen, dass aufgrund der Probleme der Konsumenten, die Qualität von Produkten oder Dienstleistungen zu beurteilen, sich eher schlechtere statt bessere Leistungen auf dem Markt durchsetzen, was unter den Stichworten »adverse Selektion« und »moral hazard« in der Ökonomie umfassend untersucht worden ist.[16] Weiterhin können natürlich auch grundlegende Informationsprobleme in Bezug auf mit dem Konsum bestimmter Produkte verbundene Risiken, wie beispielsweise Gesundheitsrisiken oder Risiken für die Privatsphäre, auftreten, die auch die Anbieter nicht (oder nur begrenzt) kennen. Aus allen diesen Informationsproblemen folgt, dass Verbraucher falsche (nämlich: nicht optimale) Konsumentscheidungen treffen können.

(2) Die zweite Gruppe von Problemen, die inzwischen in der Verbraucherpolitik gleichberechtigt neben diesen Informationsproblemen steht, bezieht sich darauf, dass aus der modernen verhaltensökonomischen Forschung bekannt ist, dass sich reale Menschen nicht immer vollständig rational verhalten.[17] Vielmehr können sie systematische Entscheidungsfehler ma-

14 Vgl. hierzu beispielsweise OECD 2010: 31–50, wo diese beiden Marktversagensarten gleichberechtigt nebeneinander die theoretischen Grundlagen der Verbraucherpolitik bilden.

15 Vgl. OECD 2010: 33 ff.; Fritsch [18]2018: 249 ff.

16 Vgl. zum Problem der adversen Selektion Akerlof 1970 (»market for lemons«); zu diesen informationsökonomischen Ansätzen gehört auch die sogenannte Prinzipal-Agent-Theorie, die das Problem thematisiert, dass ein Auftraggeber (beispielsweise ein Konsument), einen Auftragnehmer (beispielsweise einen Anbieter von Dienstleistungen) aufgrund von Informationsasymmetrien nicht vollständig kontrollieren kann.

17 Vgl. zur verhaltensökonomischen Forschung in Bezug auf das Konsumentenverhalten OECD 2010: 42 ff., Luth 2010: 41 ff.

chen, die dann bei Verbrauchern zu falschen und ihren eigenen Interessen zuwiderlaufenden Konsumentscheidungen führen. Die verhaltenswissenschaftliche Forschung hat insbesondere durch experimentelle empirische Methoden eine Anzahl von solchen sogenannten »Verhaltensanomalien« (»behavioral biases«) entdeckt, die das traditionelle Rationalitätsmodell in der Ökonomie bei Entscheidungen von Individuen stark in Frage gestellt haben. Hierzu gehören Framing-Effekte, Verlustaversion, Überschätzungseffekte, Selbstkontrollprobleme, aber auch die Verwendung von (daumenregelartigen) Heuristiken in komplexen Entscheidungssituationen sowie signifikante Probleme im Umgang mit Ungewissheit und bei intertemporalen Entscheidungen.[18] Die verhaltensökonomische Forschung hat sich inzwischen erfolgreich als eigene Subdisziplin in der Ökonomie etabliert.

Die vielfältigen Erkenntnisse aus der Forschung über diese beiden Marktversagensarten sind die Grundlage der modernen Verbraucherpolitik. Aus ökonomischer Sicht kann deshalb das normativ zu verwirklichende Konzept der Konsumentensouveränität mit dem Ziel verknüpft werden, dass Konsumenten ihre Entscheidungen rational und wohlinformiert treffen. Hieraus folgt, dass die Verbraucherpolitik mit ihren Instrumenten einen Beitrag leisten soll zur Lösung dieser Informations- und Verhaltensprobleme, um den Konsumenten zu helfen, bessere Konsumentscheidungen zu treffen. Sie will der Erhöhung der Konsumentensouveränität dienen.

In der konkreten Verbraucherpolitik sind dazu eine Vielzahl von Instrumenten entwickelt worden.[19] Zentral waren hierbei immer Regulierungen, die Anbietern Informationspflichten (beispielsweise über Inhaltsstoffe von Lebensmitteln, Risiken mit Warnhinweisen u.s.w.) auferlegen, um Informationsasymmetrien zu reduzieren, oder auch direkt Mindeststandards für die Qualität von Produkten (Inhaltsstoffe, ökologische Kriterien, Sicherheit etc.) und für die Qualifikation von Anbietern von Dienstleistungen (Ärzte, Rechtsanwälte, Handwerker etc.) einzuführen. Während Informationsregulierungen sich nur auf die Informationen über Produkte und Dienstleistungen beziehen, und damit die Konsumentensouveränität durch mehr Informationen erhöhen sollen, ohne ihre Auswahlfreiheit zu beschränken, ist es das Ziel von verbindlichen Mindeststandards bei Produkten und Dienstleistungen,

18 Für eine ausführliche Erklärung vgl. DellaVigna 2009.

19 Vgl. als kurzer Überblick Kerber 2014: 279–281; für einen breiten anwendungsorientierten Überblick OECD 2010: 77 ff.

die Sicherheit, Gesundheit und ökonomischen Interessen der Verbraucher direkt zu schützen. Allerdings kann dies zu einer Einschränkung ihrer Auswahlfreiheit führen, weil sie dann beispielsweise weniger sichere (aber billigere) Produkte nicht mehr kaufen können. Eine andere Gruppe von Verbraucherregulierungen bezieht sich auf Mindestrechte in Verbraucherverträgen (wie beispielsweise Mindestgarantiefristen), die ebenfalls eine Einschränkung der Vertragsfreiheit darstellen. Neben solchen Regulierungen versucht die Verbraucherpolitik auch eine Fülle von freiwilligen Lösungen für diese Marktversagensprobleme zu fördern, wie Zertifizierungen, freiwillige Codes of Conduct, und andere Formen der Selbstregulierung.[20] Hierzu gehören auch Verbrauchererziehung und die Bereitstellung von direkten Informationen für Verbraucher, beispielsweise durch Aufklärung über Gesundheits- oder Sicherheitsrisiken, aber auch über ihre Rechte als Verbraucher.

Insgesamt ist die Verbraucherpolitik eine der großen Säulen der Wirtschaftspolitik, die sich in vielen konkreten rechtlichen Regelungen manifestiert. Insofern ist nicht überraschend, dass sie auch in vielfältiger Weise kritisiert wird. Aus ökonomischer Sicht steht aber zu Recht die Lösung von Informations- und Rationalitätsproblemen der Konsumenten im Mittelpunkt, die in einer hochkomplexen Welt gravierend sein können. Allerdings ist fraglich, ob die vielfältigen konkreten Regulierungen immer adäquat sind. Teilweise ergeben sich Überregulierungen, teilweise werden aber auch viele Probleme nicht ausreichend gelöst, beispielsweise durch mangelnde Durchsetzung verbraucherrechtlicher Regeln. Auch der Versuch Informationsprobleme primär durch Informationspflichten zu lösen, stößt an grundsätzliche Grenzen der Informationsverarbeitungskapazitäten der Menschen (»information overload«). Wenn die faktischen Voraussetzungen für rationale und wohlinformierte Konsumentscheidungen aber nicht ausreichend hergestellt werden können, dann kann auch die Verwendung direkter Regulierungen zweckmäßig sein, selbst wenn hierdurch die Auswahlfreiheit der Konsumenten eingeschränkt wird und dies zu Paternalismusvorwürfen führen kann.

In diesem Zusammenhang ist insbesondere auf den vor 20 Jahren entstandenen Ansatz des Libertären Paternalismus (»libertarian paternalism«)

---

20 Andere Instrumente für die direkte Beeinflussung von Verbraucherverhalten sind Steuern und Subventionen, oder als extreme Form ein direktes Verbot von bestimmten Arten des Konsums (etwa bestimmte Arten von Drogen).

zu verweisen. In diesem Ansatz wurden neue sogenannte Nudging-Politiken entwickelt, die das Verhalten gerade auch von Konsumenten so beeinflussen sollen, dass sie sich nicht durch die in der Verhaltensökonomie entdeckten systematischen Entscheidungsfehler (»behavioral biases«) selbst schädigen. Die dabei entwickelten neuen verbraucherpolitischen Instrumente benutzen bewusst die Erkenntnisse der Verhaltensökonomie, um die Konsumenten zu besseren Konsumentscheidungen zu veranlassen, ohne aber die Freiheit der Konsumenten direkt zu beschränken.[21]

## 4. Zu den Problemen der Konsumentensouveränität bezüglich Daten in der digitalen Wirtschaft

### 4.1 Sammlung von Daten in der digitalen Wirtschaft und datenschutzrechtliche Einwilligungen von Konsumenten

In der digitalen Welt müssen Konsumenten nicht mehr nur über den Kauf von Konsumgütern oder Dienstleistungen entscheiden, sondern auch über die Weitergabe von Daten, beispielsweise in Form der datenschutzrechtlichen Einwilligungen in das Sammeln und Nutzen ihrer personenbezogenen Daten.

Dies ist besonders relevant in zwei Kontexten. Am bekanntesten ist sicherlich das Sammeln riesiger Mengen von personenbezogenen Daten durch die zentralen Plattformen der großen Tech-Unternehmen (Google, Facebook, Apple, Amazon). Insbesondere Google über seine Suchmaschine und Facebook über sein soziales Netzwerk haben äußerst profitable Geschäftsmodelle entwickelt: Einerseits bieten sie hierbei den Konsumenten ihre Dienstleistungen an, für die diese – ökonomisch gesehen – mit ihren personenbezogenen Daten bezahlen,[22] und andererseits verwenden sie diese Daten als zentralen Input für ihre Dienstleistung der »zielgerichteten Werbung« (»targeted advertising«), die sie an Unternehmen für Werbezwecke verkaufen. Aufgrund ihrer herausragenden Position bei der

---

21 Vgl. Sunstein/Thaler 2003, Thaler/Sunstein 2008, und als kritischer Überblick in Bezug auf Verbraucherpolitik Luth 2010: 61 ff., und Kerber 2014.

22 Juristisch versucht man den Begriff »Daten als Gegenleistung« zu vermeiden, aber aus ökonomischer Sicht ist es genau dies. Insofern ist dies auch als ein Primärmarkt für personenbezogene Daten bezeichnet worden (Schweitzer/Peitz 2017: 30 ff.).

Sammlung solcher personenbezogenen Daten sind beide Unternehmen in vielen Ländern zu den dominierenden Unternehmen in der Werbeindustrie aufgestiegen. Die im Zusammenhang mit der Diskussion um die Marktmacht dieser Unternehmen durchgeführten Studien haben gezeigt, wie stark ihre Marktstellung und ihre hohen Gewinne von der weitreichenden Sammlung und Auswertung der Daten der Konsumenten abhängig sind.[23] Neben diesen und anderen digitalen Plattformen, die aufgrund von hohen Skalenerträgen und direkten und indirekten Netzwerkeffekten auch zur Entstehung von monopolistischen Strukturen neigen, spielt die Sammlung von Daten von Konsumenten auch zunehmend im Bereich des sich rasch ausbreitenden »Internet der Dinge« (»Internet of Things«: IoT) eine zentrale Rolle. Dies bezieht sich auf alle Arten von smarten Geräten, wie beispielsweise vernetzte Autos, smarte TV-Geräte und andere Smarthome-Anwendungen (einschließlich »digital personal assistants« wie Amazon Echo mit Alexa), aber auch smarte Uhren und Fitnesstracker, die durch die Nutzung der Konsumenten eine Fülle von Daten generieren. Üblicherweise haben die Hersteller dieser Geräte eine exklusive Kontrolle über diese Daten und können sie vielfältig nutzen und monetarisieren. In Zukunft werden mit Sensoren, Mikrofonen und Kameras ausgestattete und vernetzte smarte Geräte überall vorhanden, das heißt omnipräsent sein, und damit auch überall Daten über Konsumenten sammeln und verwerten. Insofern ist die Frage der Governance dieser Daten von fundamentaler Bedeutung.

In diesem Beitrag kann nicht auf das Problem eingegangen werden, wem die bei der Nutzung einer Plattform und des eigenen Fahrzeugs oder smarten TV-Geräts generierten vielfältigen Daten »gehören« sollen, das heißt wer welche Rechte an diesen (oft auch nicht personenbezogenen) Daten haben soll.[24] Dies ist eine bislang ungeklärte und nicht durch den Gesetzgeber entschiedene Frage, für die in Bezug auf IoT-Geräte der im Februar 2022 publizierte »Data Act«-Vorschlag der Europäischen Kommission eine große Relevanz haben könnte.[25] Im Folgenden werden wir uns deshalb – wie angekün-

---

23 Vgl. zur Stellung dieser Unternehmen auf den Märkten für digitale Werbung ACCC 2019: Kap. 2.6, 2.7 und CMA 2020: Abs. 3.189–3.197.

24 Vgl. zu dem Beispiel der Daten des vernetzten Autos Kerber/Gill 2020 sowie aus einer vertieften ökonomischen Sicht Kerber 2018.

25 Vgl. Vorschlag »Data Act« (Europäische Kommission 2022b). Im abschließenden Abschnitt 5 werden wir kurz auf dieses Problem der Spezifizierung und Zuordnung der Rechte an Daten zurückkommen, und wie dieses konzeptionell mit den Begriffen Konsumentensouveränität und Datensouveränität zusammenhängt.

digt – auf die Konsumentenentscheidungen in Bezug auf personenbezogene Daten konzentrieren, für die mit der DSGVO das europäische Datenschutzrecht im Prinzip solche Rechte geklärt hat. Da die Verarbeitung personenbezogener Daten eine rechtliche Grundlage benötigt, spielt in beiden Kontexten (Plattformen und IoT) die datenschutzrechtliche »Einwilligung« der Konsumenten (als Datensubjekte) die zentrale Rolle für die Sammlung und Nutzung dieser Daten durch die Plattformen und Hersteller von IoT-Geräten. Aus ökonomischer Sicht handelt es sich dabei um einen Vertrag zwischen dem Datensubjekt und dem datensammelnden Unternehmen, in dem festgelegt wird, welche Daten gesammelt werden, mit wem diese Daten geteilt und für welche Zwecke sie genutzt werden können. Konkret findet sich dies in der spezifischen Datenschutzerklärung des datensammelnden Unternehmens (oft auch »privacy policy« genannt), in die die Konsumenten einwilligen.

Nach Art. 4 (11) DSGVO ist es notwendig, dass jede Einwilligung eine: »[…] freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung […]« ist. Wichtig ist, dass hierbei im Prinzip Vertragsfreiheit besteht: das datensammelnde Unternehmen kann beliebige personenbezogene Daten für beliebige Zwecke sammeln und diese auch mit anderen teilen. Allerdings muss es spezifisch darüber informieren, welche Daten gesammelt werden, für welche Zwecke sie benutzt werden, und mit welchen Unternehmen es diese für welche Zwecke teilt.[26] Aus verbraucherpolitischer Sicht handelt es sich damit um eine – zumindest theoretisch – sehr weitgehende Informationspflicht, die es den Konsumenten ermöglichen soll, eine wohlinformierte Entscheidung über einen solchen Vertrag zu treffen. Dies bezeichnet man auch als eine sogenannte »notice and consent«-Lösung, was konkret heißt, dass die Konsumenten informiert werden müssen und auf der Basis dieser Information dann zustimmen können. Aus ökonomischer Sicht könnte man diese Vereinbarung auch als eine Art »Lizenzvertrag« über die Nutzung der eigenen personenbezogenen Daten der Konsumenten verstehen.

Da die Entscheidungen über diese datenschutzrechtlichen Einwilligungen (fast) immer im Kontext der Nutzung von bestimmten Produkten, Dienstleistungen oder Informationsangeboten getätigt werden (mit oder ohne monetäre Bezahlung), sind sie aus ökonomischer Sicht Teil von Kon-

26 Darüber hinaus muss es auch eine Fülle weiterer Anforderungen erfüllen, beispielsweise die Rechte der Datensubjekte respektieren und die Daten sicher speichern.

sumentscheidungen. Die Anforderungen des Datenschutzrechts, dass die Konsumenten solche Einwilligungen in die Sammlung und Nutzung ihrer personenbezogenen Daten freiwillig und wohlinformiert geben können sollen, ist folglich völlig kompatibel mit dem normativen Ziel der Konsumentensouveränität, jetzt aber konkretisiert mit Blick auf die Ausübung der aus dem Datenschutzrecht folgenden Rechte der Individuen über ihre personenbezogenen Daten. Eine mögliche Ausprägung des Begriffs »Datensouveränität« könnte sich dann darauf beziehen, ob und inwieweit individuelle Personen frei und wohlinformiert darüber entscheiden können, welche »ihrer« Daten von welchen Akteuren (wie beispielsweise Unternehmen) gesammelt und für welche Zwecke genutzt werden können. Dies kann sich sowohl darauf beziehen, andere Akteure von der Sammlung und Nutzung solcher Daten auszuschließen (durch Verweigerung der Einwilligung), als auch darauf, anderen Akteuren für bestimmte Zwecke diese Daten bewusst zugänglich zu machen, beispielsweise um selbst bestimmte Dienstleistungen zu erhalten oder um Gemeinwohlinteressen zu fördern (Datenspende). Von zentraler Bedeutung ist dabei immer auch, dass die Möglichkeit von gezielt und differenziert ausgestalteten Einwilligungen auch ein zentrales Instrument der Konsumenten zum Schutz ihrer Privatsphäre ist.

## 4.2 Marktversagensprobleme bei Konsumentenentscheidungen über Einwilligungen

### *4.2.1 Einleitung*

Insofern kann nun gefragt werden, ob auf realen Märkten in der digitalen Ökonomie, beispielsweise auf digitalen Plattformen oder bei der Nutzung von IoT-Produkten, eine solche Datensouveränität, im Sinne der Konsumentensouveränität in Bezug auf Entscheidungen über personenbezogene Daten, faktisch gegeben ist oder ob hier erhebliche Probleme bestehen. In Deutschland haben beispielsweise 2019 die Wettbewerbskommission 4.0 und die Datenethikkommission diesbezüglich erhebliche Probleme diagnostiziert und von der Politik Maßnahmen gefordert, um diese Probleme zu lösen. Die Wettbewerbskommission 4.0 hat dies in ihrem Bericht auch explizit mit dem ökonomischen Begriff der Konsumentensouveränität

ausgedrückt.[27] Über diese Probleme gibt es bereits seit langem vielfältige Forschung, deren Ergebnisse im Folgenden kurz zusammengefasst und in diesen ökonomischen Rahmen eingeordnet werden sollen.

Inzwischen gibt es seit mehr als 15 Jahren eine sehr kritische Diskussion darüber, ob und inwieweit sich individuelle Nutzer in der digitalen Welt vor einer zu weitgehenden Sammlung und Nutzung ihrer Daten schützen können, gerade auch im Hinblick auf den Schutz ihrer Privatsphäre. Diese Diskussion ist zunächst auch unter dem Stichwort »privacy paradox« geführt worden, das heißt der empirischen Beobachtung des Widerspruchs, dass viele Nutzer auf der einen Seite bei Befragungen sich sehr besorgt zeigen bezüglich des Schutzes ihrer Daten, und gleichzeitig aber auf der anderen Seite in ihrem tatsächlichen Internetverhalten oft nicht auf ihre Daten achten und auch (ohne weitere Prüfung) großzügig ihre Einwilligung zur Sammlung und Nutzung ihrer Daten zu geben scheinen. Die eine mögliche Interpretation dieses Paradoxes, nämlich dass den Verbrauchern der Schutz ihrer Privatsphäre nicht wichtig ist und somit gar kein Problem besteht, wird inzwischen breit abgelehnt. Vielmehr werden in der Diskussion immer klarer die vielfältigen Hindernisse analysiert, durch die die Konsumenten unter den realen Bedingungen auf digitalen Märkten nicht mehr in der Lage sind, mit solchen Einwilligungen die Sammlung und Nutzung ihrer Daten sinnvoll zu kontrollieren und nach ihren eigenen Präferenzen zu »managen«. In diesem Zusammenhang ist immer wieder davon die Rede, dass die Konsumenten von diesen Entscheidungen überfordert sind (»overwhelmed«) und es deshalb oft faktisch aufgegeben haben, durch Lesen von Datenschutzerklärungen und Auswählen von eventuell angebotenen Optionen auf die Sammlung und Nutzung ihrer Daten Einfluss zu nehmen oder sie gar kontrollieren zu können.[28] Jeder Leser und jede Leserin kennt diese Problematik aus den eigenen Erfahrungen. Im Folgenden sollen aber die Ursachen dieser Probleme genauer analysiert werden. Aus ökonomischer Sicht können sie gut mit Hilfe der bereits in Abschnitt 3 erläuterten Marktversagenskategorien erklärt werden.

27 Vgl. Wettbewerbskommission 4.0 2019: 23 f. und 38 ff.; Datenethikkommission 2019: 95–140.
28 Vgl. hierzu Norberg u. a. 2007, Solove 2013, Kokolakis 2015, Acquisti u. a. 2020.

### *4.2.2 Informations- und Rationalitätsprobleme*

Im Mittelpunkt stehen dabei die bereits bei der Verbraucherpolitik diskutierten Informations- und Rationalitätsprobleme.[29] Seit langem ist es ein großes Problem, dass viele Unternehmen eine Fülle von Daten von Konsumenten heimlich sammeln, ohne darüber zu informieren, das heißt die Konsumenten wissen nicht, dass bzw. welche Daten über sie gesammelt werden. Selbst wenn inzwischen durch Datenschutzerklärungen Informationen gegeben werden, so sind diese Informationen über die Frage, welche Daten gesammelt werden und für welche Zwecke sie genutzt werden, oft sehr allgemein gehalten. Auf diese Weise bleiben das Ausmaß und die spezifische Verwendung ihrer Daten weitgehend intransparent für die Konsumenten. Ein anderes, bereits lange bekanntes Problem ist, dass Datenschutzerklärungen sehr umfangreiche, juristisch formulierte Texte sind, die nicht nur schwer verständlich sind, sondern auch einen ökonomisch nicht akzeptablen Zeitaufwand erfordern. Hinzu kommt, dass die gesammelten Daten oft mit vielen andere Firmen geteilt werden (mit wiederum eigenen Datenschutzerklärungen). Da die Teilnahme am digitalen Leben erfordert, ständig solche Entscheidungen zu treffen, ist es auch aus ökonomischer Sicht oft völlig rational, sich nicht um jede einzelne Datenschutzerklärung zu kümmern und Einwilligungen einfach routinemäßig anzuklicken.[30] Hinzu kommt, dass es für das individuelle Kalkül, ob man solchen Einwilligungen zustimmt, auch wichtig ist, dass Konsumenten normalerweise keine wirklichen Möglichkeiten haben, die positiven und negativen Wirkungen einer Einwilligung der Weitergabe und Nutzung ihrer Daten sinnvoll abschätzen zu können. Während der kurzfristige Vorteil der Nutzung eines Services vielleicht noch gut eingeschätzt werden kann, können die vielfältigen mittel- und langfristigen potenziellen Risiken, die auch dadurch entstehen können, dass die jeweiligen Daten mit anderen kombiniert und ausgewertet werden (etwa in Form von umfassenden Konsumentenprofilen), von den einzelnen Konsumenten überhaupt nicht abgeschätzt werden.

---

29 Vgl. zur folgenden Liste Kerber/Specht-Riemenschneider 2021: 30–33.

30 Aus ökonomischer Sicht ist es sehr missverständlich, dies als Ausdruck der »Trägheit« (»inertia«) von Konsumenten zu interpretieren, wie man das oft lesen kann. Auch wenn dabei verhaltensbedingte Effekte nicht ausgeschlossen werden können, so sind es doch primär die viel zu hohen Informationskosten, mit denen Konsumenten konfrontiert werden, die zu diesem Resultat führen.

Eine besondere Bedeutung haben in der Diskussion auch die vielfältigen verhaltensbedingten Rationalitätsprobleme. Insbesondere in Bezug auf den Schutz ihrer Privatsphäre scheinen solche Entscheidungen von Konsumenten stark von sehr konkreten Kontextbedingungen abhängig zu sein. Dies ist inzwischen – gerade auch in Bezug auf die »privacy paradox«-Problematik – durch verhaltenswissenschaftliche Forschung sehr gut bestätigt worden.[31] In jüngster Zeit sind diese Probleme durch eine völlig neue Diskussion über sogenannte »dark patterns« nochmals stärker in den Mittelpunkt gerückt. Im Abschnitt 3 haben wir gesehen, dass Verbraucherpolitik Nudging-Politiken verwenden kann, um Konsumenten zu helfen, selbstschädigendes Verhalten durch systematische Entscheidungsfehler (aufgrund von »behavioral biases«) zu vermeiden. So können etwa durch bewusstes Design einer bestimmten Wahlarchitektur die Konsumenten dazu veranlasst werden, beispielsweise eine gesündere Ernährung zu wählen. Trotz der positiven Wirkungen werden solche Politiken auch kritisch diskutiert, da sie auch als eine Art Manipulation des Verhaltens von Konsumenten interpretiert werden können, auch wenn sie formal immer noch die freie Wahl haben. Genau dieser Effekt einer bewussten manipulativen Beeinflussung, die auf verhaltenswissenschaftlichen Erkenntnissen basiert, wird nun auch bei den »dark patterns« im digitalen Bereich diskutiert. Hierbei geht es darum, dass durch ein geschicktes Design von Benutzeroberflächen von Webseiten, auf denen Optionen für Entscheidungen von Konsumenten präsentiert werden, das Verhalten von Konsumenten stark beeinflusst werden kann.[32] Dies kann sich auf Online-Käufe von Konsumenten beziehen, aber insbesondere auch auf die Beeinflussung ihrer Entscheidungen über Einwilligungen in Bezug auf das Ausmaß der Sammlung von Daten und deren Nutzung für vielfältige Zwecke. Im Unterschied zu Nudging-Politiken geht es aber hier nicht darum, systematische Entscheidungsfehler der Konsumenten zu korrigieren, sondern umgekehrt darum, die Einsichten in ihre »behavioral biases« gezielt dahingehend auszunutzen, dass Konsumenten Entscheidungen treffen, die im Interesse der digitalen Plattformen sind und nicht im Interesse der Konsumenten. Dies ist deshalb auch oft als »dark nudging« bezeichnet worden.

Konkret geht es hierbei nicht nur um die Frage von Opt-in oder Opt-out Lösungen für Einwilligungen, sondern auch um die farbliche Gestaltung der

31 Vgl. bereits früh Acquisti/Grossklags 2005, Kokolakis 2015, Acquisti u. a. 2020.

32 Vgl. zu »dark patterns« Forbrukerradet 2018, Luguri/Strahilevitz 2021, Martini u. a. 2021, Digital Regulation Project 2021: 17–24.

Einwilligungsbuttons, irreführende Gestaltungen von Wahlmöglichkeiten, oder andere vielfältige Tricks, die Konsumenten hierbei unter emotionalen und psychologischen Druck setzen sollen.[33] Von besonderer Bedeutung ist, dass gerade große digitale Plattformen, die bereits über umfangreiche Profile über Konsumenten verfügen, besonders gut in der Lage sind, insbesondere auch durch Einsatz von KI-Methoden (maschinelles Lernen), zielgerichtet auf einzelne Konsumentengruppen optimierte Entscheidungsdesigns zu gestalten, um deren Entscheidungen möglichst effektiv systematisch zu beeinflussen.[34] Zu diesen Möglichkeiten der manipulativen Verhaltensbeeinflussung in digitalen Kontexten gibt es inzwischen eine breite empirische Literatur. Sie hat auch dazu geführt, dass sowohl in den USA als auch in Europa eine Diskussion über dieses neue Phänomen der »behavioral manipulation« von Konsumenten auf digitalen Märkten begonnen hat. Hierbei wird auch darüber diskutiert, ob und wie es möglich ist, beispielsweise in der Verbraucherpolitik, diese Problematik besser zu lösen.[35]

#### *4.2.3 Marktmacht bzw. das Fehlen von Wahlmöglichkeiten*

Während diese bisher diskutierten Probleme gut zu den aus der Ökonomie bekannten zwei Marktversagenskategorien Informationsprobleme und Rationalitätsprobleme passen, kann es aber auch einen weiteren Grund für die mangelnde faktische Entscheidungsfreiheit über die Sammlung und Nutzung der eigenen personenbezogenen Daten geben: In bestimmten Kontexten gibt es für die Konsumenten manchmal keine realistischen Alternativen, sodass sie faktisch gezwungen sind, in die Sammlung und Nutzung ihrer Daten einzuwilligen.

Diese Problematik wurde mit der inzwischen berühmten Facebook-Entscheidung des Bundeskartellamts 2019 zentral thematisiert. Dies war weltweit das erste Mal, dass bestimmte Bedingungen für die Sammlung und Nutzung von personenbezogenen Daten eines Unternehmens als

33 Für eine Liste von fünf Kategorien von solchen »dark patterns« vgl. Martini u. a. 2021: 52.

34 Vgl. Digital Regulation Project 2021: 18: »[…] online platforms are in an especially good position to maximize the impact of their choice architecture. […] this is due to the combination of three related factors: (i) extensive data about individual consumer behavior; (ii) machine learning algorithms that can mine these data for relevant behavioral patterns; and (iii) A/B testing techniques that are designed to industrialize trial and error experimentation to maximize the choice architecture's effect on users.«

35 Vgl. Martini u. a. 2021, Luguri/Strahilevitz 2021.

missbräuchliche Ausnutzung einer marktbeherrschenden Stellung im Wettbewerbsrecht untersagt wurden.[36] Inhaltlich ging es dabei darum, dass Konsumenten, die das soziale Netzwerk von Facebook nutzen möchten, auch der Bedingung in der Datenschutzerklärung von Facebook zustimmen mussten, dass Facebook alle Daten, die es von anderen Facebook-Diensten sowie von vielen anderen Webseiten (und durch Online-Tracking Tools) über die betreffenden Konsumenten sammelt, in einem Facebook-Account zusammenführen darf. Dies führt zu besonders umfangreichen Konsumentenprofilen, die nicht nur ein großes Risiko für die Privatsphäre darstellen können, sondern Facebook auch einen Wettbewerbsvorsprung auf dem sehr lukrativen Markt für zielgerichtete Werbung (»targeted advertising«) verschaffen. Für unsere Diskussion hier ist entscheidend, dass das Bundeskartellamt in seiner Entscheidung der Meinung war, dass aufgrund der marktbeherrschenden Stellung von Facebook auf dem deutschen Markt für soziale Netzwerke die Konsumenten als Nutzer keine wirkliche Ausweichmöglichkeit haben und folglich »gezwungen« sind, dieser sehr weitgehenden Nutzung der von Facebook aus vielen Quellen gesammelten Daten zuzustimmen. Deshalb hat das Bundeskartellamt auch argumentiert, dass das marktbeherrschende Unternehmen Facebook gegen das Datenschutzrecht verstoßen hat, das ja die »Freiwilligkeit« der Abgabe einer solchen Einwilligung voraussetzt.[37] Die Lösung des Bundeskartellamts in seiner Entscheidung bestand dann auch darin, dass Facebook seinen Kunden eine zusätzliche Wahlmöglichkeit darüber geben muss, ob sie dieser Datenzusammenführung zustimmen oder nicht. Faktisch bedeutet dies, dass Konsumenten die Dienste des sozialen Netzwerks von Facebook auch dann nutzen können, wenn sie dieser Datenzusammenführung nicht zustimmen. Inhaltlich geht es damit um die Aufrechterhaltung eines Mindestmaßes an Wahlfreiheiten für die Konsumenten. Diese Lösung einer zusätzlichen Wahlfreiheit über die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen hat inzwischen auch Eingang

---

36 Bundeskartellamt 2019; vgl. zu diesem Wettbewerbsfall Robertson 2020, Podszun 2020 und Kerber/Zolna 2022.

37 Interessanterweise ist es im Datenschutzrecht bisher nicht geklärt, ob das Bestehen einer marktbeherrschenden Stellung ausreichend ist, damit eine gegebene Einwilligung als nicht »freiwillig« gegeben qualifiziert wird. Vgl. zu dieser Diskussion Graef/Van Berlo 2021 und Paal 2020, die eine solche Auffassung unterstützen würden, sich damit aber in der datenschutzrechtlichen Diskussion in einer Minderheitsposition befinden. Hieraus können sich spannende Grundsatzdiskussionen ergeben, was unter einer »freiwilligen« Entscheidung zu verstehen ist.

gefunden in den auf der EU-Ebene geplanten »Digital Markets Act« als eine der Verpflichtungen, die alle Gatekeeper-Plattformen erfüllen müssen.[38]

Was bedeutet ein solches Fehlen von Wahlmöglichkeiten für die Konsumentensouveränität in Bezug auf ihre Daten? Wenn die Konsumenten bezüglich ihrer Daten aufgrund faktisch fehlender Wahlfreiheiten durch das Bestehen einer marktbeherrschenden Stellung bzw. eines Monopols de facto nur mit einem einzigen Unternehmen einen Vertrag schließen können und folglich die Bedingungen dieses Unternehmens auf einer »take-it-or-leave-it«-Basis akzeptieren müssen, dann können Konsumenten ihre »Macht« als Nachfrager nicht mehr ausüben. Folglich ist ihre Konsumentensouveränität in Bezug auf ihre Daten und damit auch eine so verstandene Datensouveränität massiv eingeschränkt. Dies wird insbesondere für die Google-Suchmaschine und für das soziale Netzwerk von Facebook angenommen.[39] Insofern liegt hier aus ökonomischer Sicht primär das Problem im Fehlen eines wirksamen Wettbewerbs zwischen den digitalen Plattformen, die solche Dienstleistungen anbieten. Ökonomisch war es immer auch eine der zentralen Aufgaben des Wettbewerbs, die Freiheit von Konsumenten gegen die wirtschaftliche Macht von Anbietern zu sichern, insbesondere durch die Möglichkeit, zwischen den Angeboten verschiedener konkurrierender Unternehmen wählen zu können. Von daher kann es zu Recht auch eine Aufgabe der Wettbewerbspolitik sein, durch die Lösung dieses Marktversagens die Konsumentensouveränität bzw. Datensouveränität zu sichern.

### *4.2.4 Zwischenfazit*

Zusammenfassend haben wir drei Arten von Marktversagen auf digitalen Märkten identifiziert, die zu erheblichen Problemen für die Entscheidungen von Konsumenten über die Sammlung und Nutzung ihrer Daten auf vie-

38 Hierbei handelt es sich um den Art. 5(a) des »Digital Markets Act«, der eine generelle Verpflichtung für sogenannte Gatekeeper-Unternehmen enthält, personenbezogene Daten aus verschiedenen Quellen nur dann zusammenzuführen, wenn es dafür eine explizite zusätzliche Einwilligung der Nutzer gibt. Vgl. hierzu ausführlich Kerber/Specht-Riemenschneider 2021: 69–79; hierbei wird auch auf die intensive Diskussion eingegangen, ob Konsumenten in der Lage sind, rational und wohlinformiert eine solche Entscheidung zu treffen. Vgl. zum »Digital Markets Act« Europäische Kommission 2020c sowie als Überblick Caffarra/Scott Morton 2021, de Streel u. a. 2021.

39 Vgl. CMA 2020: Abs. 3.189-3.197, die diese als »must-have« Dienstleistungen bezeichnet, die für viele Menschen faktisch unverzichtbar sind.

len digitalen Märkten führen und damit die Konsumentensouveränität einschränken können:

(1) Informationsprobleme: Diese beziehen sich vor allem darauf, welche Daten konkret gesammelt und wie von welchen Unternehmen für welche Zwecke genutzt werden, und welche kurz- und längerfristigen Vor- und Nachteile (Privacy-Risiken etc.) damit für die Konsumenten verbunden sind. Weiterhin können die Informationskosten der Konsumenten durch Strategien gezielter Intransparenz und irreführender Informationen systematisch in die Höhe getrieben werden.

(2) Rationalitätsprobleme: Aus der verhaltensökonomischen Forschung ist wohlbekannt, dass Individuen sich nicht immer völlig rational verhalten und durch Ausnutzung ihrer »behavioral biases« auch gezielt verhaltensmäßig manipuliert werden können (zum Beispiel durch »dark patterns«).

(3) Marktmachtprobleme: Haben beispielsweise datensammelnde Plattformen hohe Marktmacht oder gar eine Monopolstellung, so ist die Auswahlfreiheit der Konsumenten stark eingeschränkt oder beseitigt, was auch zu einer übermäßigen Sammlung und Nutzung ihrer Daten führen kann (»excessive data collection«).

Wichtig ist zunächst, dass mit einer solchen Konzeptualisierung der Datensouveränität von Konsumenten ein klarer Bezug zur Ökonomie (einschließlich der Verhaltensökonomie) hergestellt wird, was es ermöglicht, sowohl für die Analyse dieser Probleme als auch für die Suche nach Lösungen auf die umfangreiche theoretische und empirische Forschung über diese seit langem bekannten Marktversagensprobleme zurückzugreifen. Selbstverständlich erfordert dies erhebliche zusätzliche Forschung in Bezug auf die vielfältigen neuartigen Ausprägungen dieser Marktversagensprobleme, die jetzt unter den neuen technologischen Bedingungen der Digitalisierung, nämlich der zentralen Rolle großer Datenmengen (Big Data), der Datenanalytik und Künstlichen Intelligenz (»machine-learning«) sowie der Entstehung von quasi-monopolistischen digitalen Plattformen entstanden sind. Gleichzeitig wird durch eine solche Konzeptualisierung auch deutlich, welche Politiken bzw. Rechtsgebiete als besonders relevant anzusehen sind, um diese Probleme für die Konsumentensouveränität in Bezug auf die Daten von Verbrauchern lösen zu helfen. Dies sind mit Blick auf Informations-

und Rationalitätsprobleme insbesondere die Verbraucherpolitik und in Bezug auf die hier besonders interessierenden personenbezogenen Daten das Datenschutzrecht,[40] während die Probleme fehlenden Wettbewerbs durch das Wettbewerbsrecht zu adressieren wären.[41] Darüber hinaus können jedoch auch andere Rechtsbereiche sowie zusätzliche spezielle Regulierungen mithelfen, die Probleme einer nicht ausreichend verwirklichten faktischen Konsumentensouveränität in Bezug auf Daten zu lösen.

#### *4.2.5 Lösungsmöglichkeiten zur Stärkung der Konsumenten- und Datensouveränität*

Nachfolgend wird in knapper Form der Stand der einschlägigen wirtschafts- und rechtspolitischen Diskussion über mögliche Lösungen dieser Probleme zusammengefasst. In einem ersten Schritt ist klar festzustellen, dass die oben analysierten großen Probleme von Konsumenten in Bezug auf Entscheidungen über die Sammlung und Nutzung ihrer Daten weitgehend ungelöst sind. Nicht nur die Wettbewerbskommission 4.0 und die Datenethikkommission, sondern auch die Bundesregierung in ihrer Datenstrategie und die Europäische Kommission in ihrer Mitteilung »A European Strategy for Data« betonen die Schwierigkeiten von Individuen, eine effektive Kontrolle über ihre Daten auszuüben, mit der Folgerung der Notwendigkeit einer entsprechenden Stärkung der Konsumenten.[42] Dies beinhaltet auch das Eingeständnis, dass die bisherigen Anstrengungen der Verbraucherpolitik und des Datenschutzrechts nicht ausreichend sind, um diese Probleme zu lösen.

In Bezug auf die ungelösten Marktmachtprobleme durch die großen digitalen Plattformen hat dies bereits zu einem in der Wettbewerbspolitik revolutionären Schritt geführt, nämlich zur geplanten Einführung einer zu-

---

40 In den USA, in der es bisher kein für die gesamte USA gültiges »privacy law« gibt, hat seit langem die Federal Trade Commission (FTC) in ihrer Funktion als Verbraucherschutzbehörde Regelungen bezüglich von Verträgen über die Sammlung und Nutzung von Daten von Konsumenten entwickelt.

41 Für die besonderen Probleme, die entstehen, wenn alle diese Marktversagensprobleme gleichzeitig auftreten, wie es bei den großen digitalen Plattformen oft der Fall ist, und welche Implikationen sich daraus für Lösungen ergeben, vgl. Kerber/Zolna 2022 und Kerber/Specht-Riemenschneider 2021. Konkret führt dies zu einer komplexen Beziehung zwischen Wettbewerbspolitik, Datenschutzrecht und Verbraucherpolitik.

42 Vgl. Wettbewerbskommission 4.0 2019: 38 ff., Datenethikkommission 2019: 133 ff., Bundesregierung 2021a: 7, Europäische Kommission 2020a: 20.

sätzlichen ex-ante Regulierung von großen Gatekeeper-Plattformen, da das bisherige traditionelle Wettbewerbsrecht als nicht mehr ausreichend in der Lage angesehen wird, die Marktmacht der großen Tech-Firmen in wirksamer Weise zu begrenzen. Eine nähere Analyse des Vorschlags zum »Digital Markets Act« der Europäischen Kommission zeigt aber, dass er nicht in ausreichender Weise Konsumenten vor einer übermäßigen Sammlung und Nutzung personenbezogener Daten schützt. Allerdings ist die (auf den Facebook-Fall des Bundeskartellamts zurückgehende) Verpflichtung von Gatekeeper-Plattformen zu einer zusätzlichen Einwilligung zur Zusammenführung von Daten (Art. 5 (a) DMA) ein Schritt in die richtige Richtung.[43]

Für die Lösung der oben diskutierten, wesentlich komplexeren Informations- und Rationalitätsprobleme von Konsumenten in Bezug auf ihre Entscheidungen über Daten gibt es bereits seit längerem eine breite Diskussion von Lösungsoptionen, die hier nur kurz skizziert werden kann. Zunächst ist festzustellen, dass ein Teil der Informationsprobleme, die auf mangelnde Transparenz über die Sammlung von Daten und deren Nutzung zurückgehen, (zumindest theoretisch) bereits gegen bestehende verbraucher- und datenschutzrechtliche Regelungen verstoßen kann; allerdings besteht diesbezüglich im digitalen Bereich ein großes Rechtsdurchsetzungsdefizit, was auch durch große Rechtsunsicherheit durch unklare rechtliche Regelungen verstärkt wird.[44] Nicht gelöst ist vor allem aber auch das Problem einer Informationsüberlastung der Konsumenten und einer inzwischen bestehenden »Einwilligungsmüdigkeit« angesichts der Notwendigkeit vieler Einwilligungen mit jeweils langen Datenschutzerklärungen. Naheliegend sind deshalb Vorschläge, den Informationsaufwand der Konsumenten durch Einführung von Instrumenten zu reduzieren, die es leichter machen, datenschutzfreundliche und die Privatsphäre schützende Datenschutzerklärungen zu identifizieren. Dies kann beispielsweise geschehen durch (aus der Lebensmittelkennzeichnung bekannte) Ampellösungen, »privacy icons«, datenschutzbezogene Zertifizierungen, oder durch sogenannte »one-pagers«, die in knapper übersichtlicher Form die für die Einwilligungsentscheidung wesentlichen Parameter von Datenschutzerklärungen in einer standardisierten Weise zusammenfassen und damit

43 Vgl. Caffarra/Scott Morton 2020, Kerber/Specht-Riemenschneider 2021: 69 ff.

44 Vgl. zum Problem der Rechtsunsicherheit und mangelnden Durchsetzung des Datenschutzrechts Kerber/Specht-Riemenschneider 2021: 96–108 (mit weiterer Literatur).

auch vergleichbar machen.[45] Jedoch sind auch solche Lösungen bisher nicht umgesetzt worden.[46]

Allerdings ist es sehr unklar, ob solche primär auf Information und Informationskostenreduktion bezogene Instrumente ausreichen würden, um diese Probleme zu lösen, oder ob nicht wesentlich weitergehendere Lösungen benötigt werden. Besonders viel wird dabei über Intermediäre und Datentreuhänder diskutiert, die den Konsumenten bei ihren Einwilligungsentscheidungen helfen könnten. Dies steht auch in unmittelbarem Zusammenhang mit der Diskussion um die sogenannten »Personal Information Management Systems« (PIMS), die bereits seit längerem diskutiert werden.[47] Die Grundidee solcher Lösungen besteht darin, dass diese Intermediäre Dienstleistungen anbieten, die den Konsumenten ein besseres Management ihrer Daten ermöglichen. Hierbei geht es insbesondere auch um das Management ihrer Einwilligungen, weil Konsumenten bisher keinen Überblick haben, wem sie für welche Zwecke welche Daten zur Verfügung gestellt haben und mit wem diese die Daten teilen. Solche PIMS-Lösungen können insbesondere den Konsumenten auch helfen, ihre ihnen nach der DSGVO zustehenden Rechte auszuüben und durchzusetzen, beispielsweise das Recht auf Zugang zu ihren Daten oder ihr Datenportabilitätsrecht. Aus unserer Analyse folgt aber auch, dass diese Intermediäre auch die Aufgabe haben sollten, den Konsumenten zu helfen, ihre Informationsprobleme zu lösen. Zurzeit werden solche Datenintermediäre (oft unter der Bezeichnung Datentreuhänder) viel diskutiert, auch wenn es diesbezüglich bisher keine tragfähigen Lösungen gibt. Ein zentrales ungelöstes Problem ist das Fehlen eines profitablen Geschäftsmodells, sodass eventuell über Subventionslösungen nachgedacht werden muss. Zum anderen aber ist es notwendig, durch grundlegende Regulierungen die Voraussetzungen für funktionsfähige PIMS-Lösungen zu schaffen.[48] Die Lösungen im jetzt bald in Kraft

---

45 Eine bessere Vergleichbarkeit von Datenschutzerklärungen ist von großer Bedeutung, weil ohne diese kein Wettbewerb um einen besseren Schutz der Privatsphäre bzw. datenschutzfreundlichere Produkte und Dienstleistungen möglich ist.

46 Vgl. zu solchen Lösungsvorschlägen beispielsweise Efroni u. a. 2019, Kettner u. a. 2020. Was ebenfalls regelmäßig vorgeschlagen wird, ist eine Stärkung der digitalen Kompetenzen von Individuen (Bundesregierung 2021: 40–47), was sehr an alte verbraucherpolitische Konzepte der Aufklärung und Erziehung von Verbrauchern erinnert.

47 Vgl. hierzu European Data Protection Supervisor 2016, Wettbewerbskommission 4.0, 2019: 43 f., Datenethikkommission 2019: 133 ff., Blankertz 2020, Krämer 2020: 19–28.

48 Vgl. hierzu ausführlich Specht-Riemenschneider/Kerber 2022: 24–44.

tretenden »Data Governance Act« sind diesbezüglich als unzureichend anzusehen.[49]

### *4.2.6 Fazit*

Zusammenfassend ist festzustellen, dass zurzeit nicht absehbar ist, ob die massiven Einschränkungen der Konsumentensouveränität in Bezug auf ihre Entscheidungen über die Sammlung und Verwendung der personenbezogenen Daten der Konsumenten durch die diskutierten Lösungsansätze signifikant reduziert werden können. Dies gilt vor allem für die Informations- und Rationalitätsprobleme der Konsumenten. Allerdings ist es auch sehr fraglich, ob selbst die großen Reformschritte in der Wettbewerbspolitik (beispielsweise mit dem »Digital Markets Act«) ausreichen werden, das Marktmachtproblem großer Plattformen in Bezug auf die Sammlung und Nutzung personenbezogener Daten von Konsumenten zu lösen. Zusätzlich zu diesen Marktversagensproblemen kommen jedoch noch weitere Probleme dazu, die hier nur kurz aufgezählt werden können:

(1) Eine besondere Problematik stellen Hindernisse im Datenschutzrecht selbst dar. So ist es strittig, ob Intermediäre im Auftrag von Konsumenten auch Einwilligungen abgeben können, oder inwieweit auch breitere Einwilligungen (»broad consent«) möglich sind. Hierdurch könnten Intermediäre Konsumenten besser bei diesen Entscheidungen entlasten.[50]

(2) Ein anderes Marktversagensproblem sind sogenannte externe Effekte (oder Externalitäten), die bei der Weitergabe und Nutzung von personenbezogenen Daten auf die Privatsphäre von anderen Personen auftreten. Durch die Analyse von personenbezogenen Daten einer begrenzten Anzahl von Personen einer bestimmten Gruppe können sehr weitgehende Einsichten über andere Personen dieser Gruppe gewonnen werden, die gar nicht in die Sammlung und Nutzung ihrer Daten eingewilligt haben (»inferred data«). In der ökonomischen Forschung wurde gezeigt, dass hierdurch nicht nur direkte negative externe Effekte auf die Privatsphäre anderer Individuen

---

49 Vgl. Europäische Kommission 2020b.

50 Vgl. zu diesen datenschutzrechtlichen Problemen beispielsweise Specht-Riemenschneider/Kerber 2022: 35–37.

auftreten können,[51] sondern dass hierdurch auch insgesamt auf den Märkten ein zu geringer Schutz der Privatsphäre entsteht.[52] Insofern kommt es bereits durch diesen Effekt zu einem Marktversagen in dem Sinne, dass die Präferenzen der Konsumenten hinsichtlich des Schutzes ihrer Privatsphäre systematisch nicht erfüllt werden. Dies ist nicht nur eine ökonomische Ineffizienz, sondern kann auch als eine erhebliche Einschränkung der Konsumentensouveränität in Bezug auf Daten und Privatsphäre verstanden werden. Dieses Marktversagensproblem in Bezug auf den Schutz der Privatsphäre wird erst seit kurzem in der Ökonomie untersucht; bisher gibt es auch hierfür keine konkreten Lösungsvorschläge.

## 5. Konsumentensouveränität und Datensouveränität – einige weitergehende Perspektiven aus ökonomischer Sicht

Was haben wir in diesem Beitrag gemacht? Am Beispiel der Entscheidungen über die datenschutzrechtliche Einwilligung in die Sammlung und Verwendung ihrer personenbezogenen Daten haben wir gezeigt, dass es auf realen digitalen Märkten eine ganze Anzahl von schwierigen Problemen gibt, die die faktische Konsumentensouveränität von Verbrauchern in Bezug auf ihre personenbezogenen Daten erheblich einschränken. Dies gilt dann auch für eine solchermaßen konzeptualisierte Datensouveränität der Konsumenten. Wichtig ist, dass eine solche Konzeptualisierung auch konsistent ist mit der frühen Diskussion über Konsumentensouveränität in der Ökonomie (im Anschluss an William Harold Hutt) und ihrer Betonung der »Macht« von Konsumenten, die ihnen durch ihre aktive Rolle auf der Nachfrageseite von Letztverbrauchermärkten über die Verwendung der Ressourcen einer Volkswirtschaft zukommt. Da die Daten der Konsumenten selbst eine Ressource in der Datenökonomie darstellen, über die die Konsumenten nach ihren eigenen Präferenzen entscheiden sollen (ebenso wie über ihre Arbeitskraft), sind die Marktversagensprobleme, die durch diese Einschränkungen der Konsumentensouveränität in Bezug auf ihre Daten entstehen,

51 Das Marktversagen durch negative externe Effekte spielt üblicherweise eine große Rolle in der Umweltpolitik, beispielsweise in Bezug auf $CO_2$-Emissionen, die bei der Produktion oder dem Konsum von Gütern auftreten. Vgl. zu diesem Marktversagen Fritsch [18]2018: 142 ff.

52 Vgl. Choi u. a. 2019, Acemoglu u. a. 2020.

nicht nur ein Problem für die Konsumenten, sondern auch ein Problem für die Funktionsfähigkeit von Märkten und damit der marktwirtschaftlichen Ordnung.[53]

Eine wichtige und zunehmend diskutierte Frage zielt auf die Schlussfolgerungen ab, die sich ergeben, wenn diese Marktversagensprobleme in Bezug auf personenbezogenen Daten nicht oder nur sehr begrenzt lösbar sind. Es stellt sich dann zweifellos die viel fundamentalere Frage, ob solche individuellen Entscheidungen über Daten überhaupt noch als ein geeignetes Instrument für den Schutz der Privatsphäre bzw. die Verwendung dieser Daten angesehen werden können. Wenn das Instrument der individuellen Einwilligung faktisch als Steuerungsinstrument für den Schutz der Individuen und die Verwendung der Daten nicht ausreichend funktioniert, so wird man sich Gedanken machen müssen, ob man den Bereich »souveräner« individueller Entscheidungen einschränkt und dann durch politische oder regulatorische Entscheidungen bestimmt, unter welchen Umständen welche Daten für welche Zwecke vom wem gesammelt und verwendet werden können. Datenschutzrechtlich würde dies bedeuten, dass man den Anwendungsbereich der Einwilligung nach Art. 6 (1)a DSGVO verkleinert. Dies könnte bedeuten, dass man dann einerseits für bestimmte Arten von personenbezogenen Daten unter bestimmten Bedingungen und für bestimmte Zwecke (beispielsweise Forschungszwecke) die Sammlung und Nutzung solcher Daten direkt erlaubt, ohne dass noch eine Einwilligung erforderlich ist. Andererseits könnte das auch implizieren, dass in anderen Kontexten das Sammeln und/oder die Verwendung von bestimmten personenbezogenen Daten generell verboten wird, weil dies mit besonders großen Risiken verknüpft ist oder weil in bestimmten Entscheidungskontexten die Fähigkeiten der Konsumenten in besonderer Weise eingeschränkt sind, rationale wohlinformierte Entscheidungen zu treffen. Man sollte dabei sehr vorsichtig sein, solche Entscheidungen nicht zu voreilig mit dem Paternalismusvor-

53 Uns ist bewusst, dass in der EU der Schutz der informationellen Selbstbestimmung bzw. der Privatsphäre ein Grundwert ist, der normativ nicht auf ein ökonomisches Effizienzkalkül reduziert werden kann (vgl. Kerber 2016: 645). Dies ändert aber nichts daran, dass die hier verwendeten Marktversagensanalysen wichtige Beiträge für die Analyse der Probleme für freie, rationale und wohlinformierte Entscheidungen der Konsumenten über ihre Daten und der zur Verfügung stehenden Lösungsmöglichkeiten leisten können.

wurf zu diskreditieren, da es auch im Sinne der Konsumenten selber sein kann, vor bestimmten Gefahren geschützt zu werden.[54]

Mit dieser Frage über die Größe und die konkrete Definition des Bereichs, innerhalb dessen freie individuelle Entscheidungen über personenbezogene Daten möglich sein sollen, und wie – durch generelle Erlaubnisse oder Verbote der Sammlung und Nutzung von Daten – dieser Bereich der Relevanz von individuellen »Einwilligungen« begrenzt sein soll, wird eine andere zusätzliche Dimension der Datensouveränität angesprochen: Es geht hierbei um die Frage, über welche Daten (und unter welchen Bedingungen) Personen überhaupt individuelle Entscheidungsrechte haben sollten. In unserem Beitrag haben wir bewusst unsere Diskussion über die Ausübung von »souveränen« Entscheidungen auf diejenigen Rechte an personenbezogenen Daten bezogen, für die in der DSGVO eine »Einwilligung« benötigt wird. Tatsächlich ist die Einwilligung nach Art. 6 (1)a DSGVO aber nur eine von mehreren Rechtsgrundlagen, auf deren Basis eine Verarbeitung von personenbezogenen Daten möglich ist. Beispielsweise ist eine solche Verarbeitung auch ohne Einwilligung nach Art. 6 (1)f DSGVO möglich, wenn die »berechtigten Interessen« eines Unternehmens an der Verarbeitung dieser Daten größer sind als das Interesse des Datensubjekts am Schutz seiner oder ihrer Privatsphäre. Mit dieser und anderen Regeln enthält das Datenschutzrecht bereits eine Fülle von sehr differenzierten Regeln, mit denen Interessenabwägungen möglich sind, durch die die Rechte der Individuen über ihre personenbezogenen Daten auch stark begrenzt werden können. Hiermit sind wir – ökonomisch und rechtlich gesehen – auf der Ebene der Spezifizierung und Zuordnung eines Bündels von Rechten, welches das Datensubjekt und andere Akteure (einschließlich des Staates) an der Nutzung von personenbezogenen Daten dieses Datensubjekts haben können.[55] Die Frage nach der Datensouveränität von Konsumenten beinhaltet folglich auch die Dimension der Größe und der konkreten Ausgestaltung des Bündels von Rechten, das diese Individuen über ihre personenbezogenen Daten haben. Dieses Bündel von Rechten kann größer

---

54 Vgl. Kerber 2014: 292 f. zur Idee, dass Konsumenten selbst Interesse an bestimmten paternalistisch interpretierbaren Einschränkungen ihrer Entscheidungsfreiheit haben können, um besser gegen bestimmte Risiken (wie beispielsweise Privacy-Risiken) geschützt zu sein, und deshalb solche Lösungen politisch unterstützen könnten. Ein solcher Ansatz des »Selbstpaternalismus« kann insbesondere auch aus einer konstitutionenökonomischen Perspektive begründet werden (Kerber/Vanberg 2001: 67–79).

55 Vgl. zur Anwendung des »bundles of rights«-Ansatzes auf Daten Kerber 2022.

oder kleiner ausgestaltet sein, ebenso wie auch andere Akteure in größeren oder kleineren Umfang Rechte an der Nutzung dieser personenbezogenen Daten dieses Datensubjekts haben können.

Abschließend soll in Bezug auf die Datensouveränität von Konsumenten ebenfalls darauf hingewiesen werden, dass Konsumenten auch Entscheidungsrechte über die Sammlung und Nutzung von nicht personenbezogenen Daten haben können. Beispielsweise ist in Australien der Ansatz der sogenannten »consumer data rights« entwickelt worden, in dem Konsumenten Rechte (beispielsweise auch Datenportabilitätsrechte) über die Nutzung ihrer »consumer data« zugewiesen werden. Der Begriff der »consumer data« ist dabei unabhängig vom australischen »privacy law« definiert und kann auch nicht personenbezogene Daten umfassen.[56] Solche Rechte von Konsumenten an nicht personenbezogenen Daten werden auch zunehmend in der EU durch zusätzliche spezielle gesetzliche Regelungen eingeführt. Beispielsweise findet sich im Vorschlag zum »Digital Markets Act« der Kommission ein neues spezifisches Datenportabilitätsrecht (Art. 6 (1)h) für Konsumenten als Endnutzer von Plattformdiensten von Gatekeepern (beispielsweise als Endnutzer der Amazon Online-Shopping-Plattform) in Bezug auf die Daten, die sie selbst in ihren Interaktionen mit Händlern auf der Plattform generiert haben. Dieses Portabilitätsrecht bezieht sich dabei explizit auch auf nicht personenbezogene Daten und geht damit weit über das datenschutzrechtliche Datenportabilitätsrecht (Art. 20 DSGVO) hinaus.[57] Wesentlich bedeutender könnten aber die Auswirkungen des kürzlich publizierten Vorschlags zum »Data Act« der Europäischen Kommission sein: Konsumenten als Nutzer von IoT-Geräten würden dann ein Datenzugangs- und Datenteilungsrecht für alle auf IoT-Geräten generierten Daten bekommen. Dies würde gerade auch die nicht personenbezogenen IoT-Daten umfassen.[58] Dies bedeutet, dass sich die Datensouveränität von Konsumenten auch auf viele nicht personenbezogene Daten beziehen kann, wodurch auch datenrechtliche Regelungen außerhalb des Datenschutzrechts sehr relevant sein können. Allerdings ergeben sich auch hier bei den Entscheidungen über die Sammlung und Nutzung der

---

56 Vgl. OECD 2020: 7–14.

57 Vgl. Kerber/Specht-Riemenschneider 2021: 81–85.

58 Vgl. Art. 4 (Datenzugangsrecht der Nutzer) und Art. 5 (Datenteilungsrecht mit Dritten, insbesondere Dienstleistungsanbietern) des »Data Act«-Vorschlags der Europäischen Kommission (2022b).

nicht personenbezogenen Daten der Konsumenten im Prinzip die gleichen Marktversagensprobleme wie bei den oben ausführlich diskutierten datenschutzrechtlichen Einwilligungen bezüglich der personenbezogenen Daten.[59]

59 Es ist eines der zentralen Probleme des »Data Act«-Vorschlags der Europäischen Kommission, dass er diese Marktversagensprobleme nicht adressiert.

# Datensouveränität zwischen informationeller Selbstbestimmung und EU-Datenschutzgrundrecht

*Kevin Ferber*

Die Debatte über den Umgang mit personenbezogenen Daten entfernt sich zunehmend vom Leitbegriff des Datenschutzes und entwickelt sich entlang neuer, miteinander um die Position des Leitbegriffs konkurrierender Konzepte. Eines dieser Konzepte ist die Datensouveränität. Der nachfolgende Beitrag wählt eine rechtswissenschaftliche Perspektive und legt den Fokus dabei auf das Verfassungsrecht sowie die Ausgestaltung des Grundrechtsschutzes. Er möchte zeigen, weshalb die Datensouveränität als »verantwortliche informationelle Freiheitsgestaltung« (Deutscher Ethikrat 2018: 252) vom Ausgangspunkt der informationellen Selbstbestimmung nach dem Grundgesetz weniger aufwendig zu begründen ist als aus der Richtung des Datenschutzgrundrechts in Art. 8 der europäischen Grundrechtecharta, auf der das bestehende Datenschutzrecht der DSGVO fußt.

## 1. Datensouveränität als informationelle Freiheitsgestaltung

Datensouveränität wird zum einen als – dann negativ konnotierter – politischer Kampfbegriff in der Debatte über die Zukunft des Umgangs mit personenbezogenen Daten genutzt, der aus Sicht vieler Datenschützer gelesen wird als der Versuch, »Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern« (Datenschutzkonferenz 2017a: 1). Diese etwa mit Blick auf eine »Datenökonomie« (BMWi 2016: 33) durchaus feststellbaren Verwendungen des Begriffs, die als »Versuche, eine Ökonomisierung des Datenschutzes zu erreichen und das Prinzip ›Dienst gegen Daten‹ zu etablieren« (Hornung/Spiecker gen. Döhmann 2019: 310), verstanden werden können, gehen eher in die Richtung eines Dateneigentums. Sie deuten die Datensouveränität

also im Sinne einer absoluten Verfügungsbefugnis über die eigenen Daten, bis hin zu einer Möglichkeit der Veräußerung personenbezogener Daten. (vgl. Hoeren 2013: 486; Zech 2015b: 137; Fezer 2017a: 99).

Demgegenüber verwendet der Deutsche Ethikrat in seiner Stellungnahme *Big Data und Gesundheit* aus dem Jahr 2017 eine andere Lesart von Datensouveränität. Als »eine den Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung« baut es auf der informationellen Selbstbestimmung auf und sieht sich als »interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt« (Deutscher Ethikrat 2018: 252). Diese Privatheit dürfe hierbei nicht »allzu starr und statisch im Sinne eines (dauerhaft) abgeschlossenen Raumes« (ebd.) ausfallen. Um Datensouveränität zu verwirklichen, müsse der Einzelne nach persönlichen Präferenzen in den Strom persönlich relevanter Daten eingreifen können (ebd.: 253). Jedoch solle diese Freiheitsgestaltung nicht dazu dienen, den durch den herkömmlichen Datenschutz etablierten Schutz der Person zu schwächen oder gar zu schleifen. Die Datensouveränität solle dazu dienen, neben dem Individuum auch die Bedeutung von Daten für die Gesellschaft als soziale Ressource hervorzuheben. Daten dürften »nicht allein als wichtiges individuelles Gut verstanden, sondern [müssten] auch in ihrer kollektiven Dimension verstanden werden.« (vgl. ebd.: 253)

Aus der verfassungsrechtlichen Sicht ist dieser Ansatz vor allem deshalb interessant, weil die vorgeschlagene Stoßrichtung die Bedeutung von Daten als gesellschaftliches Phänomen in den Vordergrund rückt, auch wenn dafür die vor allem durch das Europarecht starke Fokussierung auf den Schutz der Privatsphäre abgeschwächt werden muss. Dieser Zusammenhang verdient eine nähere Betrachtung. Es gilt also darzustellen, wie sowohl die gesellschaftliche Komponente in der von der Stellungnahme aufgegriffenen Vorstellung von informationeller Selbstbestimmung wirkt als auch, weshalb der Schutz der Privatsphäre im EU-Datenschutzgrundrecht einen solch hohen Stellenwert einnimmt.

## 2. Die informationelle Selbstbestimmung als Ausgangspunkt der Datensouveränität

Im deutschen Verfassungsrecht des Grundgesetzes gibt es kein ausdrückliches Recht auf Datenschutz. Zur Zeit der Entstehung des Grundgesetzes war die heutige Massendatenverarbeitung mit Hilfe von Computern noch nicht vorstellbar, geschweige denn vorhersehbar. Dass ein Grundrecht auf Datenschutz auch in späteren Jahren nicht in den Wortlaut des Gesetzes ergänzt wurde, lässt sich auf die aktive Rolle des Bundesverfassungsgerichts (BVerfG) zurückführen, das im Rahmen der richterlichen Rechtsfortbildung insbesondere für den Bereich der freien Persönlichkeitsentfaltung in Art. 2 Abs. 1 GG die Notwendigkeit eines weitergehenden Schutzes bereits erkannt und schon 1980 auch ausformuliert hat. Das allgemeine Persönlichkeitsrecht ist darauf ausgerichtet,

> »im Sinne des obersten Konstitutionsprinzips der ›Würde des Menschen‹ (Art. 1 Abs. 1 GG) die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen; diese Notwendigkeit besteht namentlich auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit.« (BVerfGE 54, 148, 153)

Das allgemeine Persönlichkeitsrecht sichert als unbenanntes Freiheitsrecht, nämlich aus der Zusammenschau von Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, die persönliche Autonomie nach innen und außen. Insbesondere geht der Schutz auch auf Konstellationen ein, die vom Verfassungsgeber nicht vorhergesehen werden konnten, die aber dennoch einen Schutz der Persönlichkeit notwendig machen (vgl. Dreier 2013: 69). Die Menschenwürdegarantie des Art. 1 Abs. 1 GG dient dabei als programmatische Leitlinie und Maßstab für eine strenge Verhältnismäßigkeitsprüfung (vgl. ebd.). Dieser Integritätsschutz des allgemeinen Persönlichkeitsrechts ist von der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG abzugrenzen, die als Auffanggrundrecht einen umfassenden Aktivitätsschutz bietet (vgl. ebd.).

Das allgemeine Persönlichkeitsrecht umfasst wiederum als Teilfälle neben dem gleich näher zu betrachtenden Recht auf informationelle Selbstbestimmung auch den Schutz von Intim- und Privatsphäre, den Namens- und Ehrschutz, das Recht auf Selbstdarstellung und die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. Eifert 2015: 1181 ff.; Jarass 1989: 857; Britz 2007: 68; Schöndorf-Haubold 2020: 32 ff.).

Das Recht auf informationelle Selbstbestimmung wurde durch das BVerfG in seiner Entscheidung zum damals zum Zweck einer bevölkerungsweiten Datenerhebung erlassenen, politisch umstrittenen Volkszählungsgesetz 1983 als Ausprägung des allgemeinen Persönlichkeitsrechts gefasst, um unter den Bedingungen der modernen Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu gewährleisten (vgl. BVerfGE 65, 1; vgl. Peilert 2017: 371 ff.).

Eingangs macht das BVerfG in seiner Entscheidung klar, dass die Befugnis, »grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden« (BVerfGE 65, 1, 42), vom allgemeinen Persönlichkeitsrecht umfasst ist. Insbesondere durch die automatische Datenverarbeitung sei diese Befugnis jedoch unter Druck geraten, weshalb es zur Umsetzung dieser individuellen Selbstbestimmung »unter den Bedingungen moderner Informationsverarbeitungstechnologien« (ebd.) auch tatsächlicher Entscheidungs- und Verhaltensmöglichkeiten bedürfe. Sonst drohe eine Hemmung der Freiheitsausübung, wenn der Einzelne nicht mehr wisse, welche Informationen seinem sozialen Umfeld und seinen Kommunikationspartnern bekannt sind (vgl. ebd.: 43). Neben den »individuellen Entfaltungschancen des Einzelnen« wäre auch das Gemeinwohl gefährdet, »weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens« sei (ebd.). Daraus schließt das BVerfG:

> »Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.« (BVerfGE 65, 1, 43)

Diese Konzeption hat dem BVerfG den Vorwurf eingebracht, dass es sich bei der informationellen Selbstbestimmung ausschließlich um eine eigentumsanaloge Verfügungsbefugnis handele, die die selbstbestimmte Teilhabe an Kommunikationsprozessen nicht berücksichtige (Simitis 1987: 1491; Hoffmann-Riem 1998: 521). Die somit vermutete »Vernachlässigung der sozialen Dimension von Information« (Britz 2010: 566) lässt sich konkretisieren, wenn man sich vergegenwärtigt, dass die eigentlich für den Grundrechts-

schutz relevante Beeinträchtigung nicht in der Erhebung von Daten liegt, sondern »aus der Antizipation wie auch immer gearteter nachteiliger Entscheidungen, die an bestimmte informationsbedingte Vorstellungen der anderen von der eigenen Person anknüpfen« (ebd.: 567). Erst dieser soziale Kontext mache die Preisgabe von Daten zu einer Bedrohung für die Freiheit des Individuums, vor dem auch die informationelle Selbstbestimmung dann ebenso schützen müsse. Ein Datenverfügungsrecht sei deshalb lediglich ein Instrument zum Schutz vor den Gefahren eines nicht regulierten Umgangs mit Daten (ebd.: 568). Statt auf eine Datenverfügungsbefugnis müsse die informationelle Selbstbestimmung auf die »Sicherung der Verhaltensfreiheit« mit Blick auf die »aus der Daten- und Informationsverwendung durch andere drohenden Freiheitsbeeinträchtigungen« (ebd.: 573) gerichtet sein. Diese Ansicht stellt also klar, dass die informationelle Selbstbestimmung zum einen nicht dem Schutz der Daten um ihrer selbst willen dient und zum anderen auf die Gewährleistung der freien Persönlichkeitsentfaltung im Sinne des Art. 2 Abs. 1 GG ausgerichtet ist.

Das Verständnis von Datensouveränität des Deutschen Ethikrates wiederum fußt, wie bereits oben zitiert, auf einer Fortentwicklung der informationellen Selbstbestimmung hin zu einer informationellen Freiheitsgestaltung (Deutscher Ethikrat 2018: 252). Der Deutsche Ethikrat widmet sich in seinen Überlegungen denn auch selbst ausführlich der informationellen Selbstbestimmung. Er attestiert dem Volkszählungsurteil eine »missverständliche Formulierung, die das Recht auf informationelle Selbstbestimmung eigentumsähnlich erscheinen lässt« (ebd.: 125). Auch sei »gegenüber verbreiteten Fehldeutungen zu betonen, dass das Recht auf informationelle Selbstbestimmung auch die Befugnis umfasst, selbst zu bestimmen, mit welchen Inhalten und in welchen Beziehungen jemand in den Prozess interaktiver Persönlichkeitsentfaltung mit seiner Umwelt eintritt« (ebd.: 126). Dass dies sowohl für das deutsche wie für das europäische Verfassungsrecht gelte, wird mit einem Verweis auf einen Aufsatz von Klement (vgl. Klement 2017: 169) dargelegt und gibt hier die Gelegenheit, das europäische Datenschutzgrundrecht des Art. 8 GRCh und das Verständnis von informationeller Selbstbestimmung im EU-Primärrecht zu betrachten. Der konzeptionellen Kritik am Volkszählungsurteil schließt der Ethikrat sich nicht ausdrücklich, aber doch implizit ebenfalls an, da sein Verständnis von informationeller Selbstbestimmung viele der genannten Punkte aufgreift, dabei aber unterstellt, dass dies der Rechtsprechung des BVerfG ohnehin zu

entnehmen sei (vgl. Deutscher Ethikrat 2018: 125; vgl. auch Hoffmann-Riem 1998: 521).

## 3. Die Grundlagen des bestehenden Datenschutzes im europäischen Primärrecht

Um die Frage wieder aufzugreifen, ob das EU-Primärrecht ein Recht auf informationelle Selbstbestimmung kennt, ist zunächst festzustellen, dass aufgrund der unmittelbaren Geltung der europäischen DSGVO sich auch der Grundrechtsschutz im Bereich des Datenschutzes weitgehend nach dem EU-Primärrecht richtet und diesem deshalb ein besonderes Augenmerk zukommen muss. Das Datenschutzrecht in Europa ist durch die Einführung der DSGVO weitgehend auf ein einheitliches Schutzniveau gebracht, aber auch grundbegrifflich und systematisch vereinheitlicht worden. Nach Art. 288 Abs. 2 AEUV gilt eine Verordnung unmittelbar in allen Mitgliedstaaten der EU. Die Bedeutung der bundesdeutschen Datenschutzgesetze ist dadurch geschrumpft auf die Ausgestaltung von Regelungen, die die DSGVO den Mitgliedstaaten in ca. 70 Öffnungsklauseln überlässt (vgl. Roßnagel 2017: 49). Auch die Datenschutzgesetze der Bundesländer beschränken sich nun auf die Regelungen der Materien, die die DSGVO explizit offenhält. Diese richten sich nach der Kompetenzordnung des Grundgesetzes und insbesondere nach den optionalen Öffnungsklauseln in Art. 6 Abs. 2 und Abs. 3 DSGVO (vgl. Hornung/Spiecker gen. Döhmann 2019: 285).

Dieser Bedeutungsverlust für das nationale Datenschutzrecht stellt sich jedoch auf den zweiten Blick weniger umfassend dar. Über die Datenschutz-Richtlinie 95/46/EG wurde in der EU seit 1995 das Datenschutzrecht schrittweise harmonisiert, denn eine Richtlinie hat zwar im Gegensatz zu einer Verordnung keine unmittelbare Geltung in den Mitgliedstaaten, allerdings verpflichtet sie die Gesetzgeber der Mitgliedstaaten gemäß Art. 288 Abs. 3 AEUV zum Erlass von Rechtsnormen, die die Richtlinie umsetzen. Die Umsetzung der Richtlinie wurde zwar in vielen Mitgliedstaaten nur zögerlich angegangen, aber die Spielräume der Mitgliedstaaten wurden durch die laufende Rechtsprechung des EuGH immer weiter verengt (vgl. Simitis/Hornung/Spiecker gen. Döhmann 2019: 147). Aufgrund der unmittelbaren Geltung der DSGVO richtet sich auch der Grundrechtsschutz im Bereich des Datenschutzes weitgehend nach dem Mehrebenensystem der EU. Hierbei

handelt es sich um das Zusammenwirken von Europäischer Menschenrechtskonvention (EMRK) und der EU-Grundrechtecharta (GRCh) sowie Normen des Sekundärrechts.

Die Herleitung des Rechts auf Datenschutz nach Art. 8 GRCh hängt eng mit dem Art. 8 EMRK zusammen, der festlegt: »Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz«, und dem der Europäische Gerichtshof für Menschenrechte (EGMR) in Ermangelung eines speziellen Grundrechts in ständiger Rechtsprechung auch ein Recht auf den Schutz personenbezogener Daten zuordnet (vgl. EGMR 1997: 95 ff.).

Diese Verbindung zu Art. 8 EMRK zeigt, dass das Datenschutzgrundrecht auf der Ebene des Unionsrechts als Frage der Privatheit behandelt wird. Der EuGH sieht auch weiterhin zwischen dem Datenschutzgrundrecht des Art. 8 GRCh und dem Anspruch auf Achtung des Privat- und Familienlebens einen »engen Zusammenhang« (EuGH 2010: 47).

Art. 8 Abs. 1 GRCh lautet: »(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.« Dieser Wortlaut lässt zunächst darauf schließen, dass es sich um ein reines Abwehrrecht gegenüber fremder Kenntnisnahme handelt. Mit Blick auf den Ursprung im Schutz der Privatsphäre und dem engen Zusammengehen mit Art. 7 GRCh lässt sich dieses Bild noch verfestigen. Umfasst sei »vor allem die *Herrschaft über die eigenen Daten*, und damit die Möglichkeit, Dritte von der Erhebung oder Verwendung dieser Daten auszuschließen.« (Kingreen 2022: 10) Dies wäre ein vorrangig auf den Schutz der Privatsphäre ausgerichtetes eigentumsanaloges Verfügungsrecht.

Jedoch ist davon auszugehen, dass es sich bei Art. 8 Abs. 1 GRCh ebenfalls um eine Form der informationellen Selbstbestimmung im Sinne eines Teilbereichs des allgemeinen Persönlichkeitsrechts handeln muss. Um dies zu begründen, beruft man sich auf die enge Verbindung zu Art. 8 EMRK, für die der EGMR festgestellt hat, dass dieser auch Aspekte des allgemeinen Persönlichkeitsrechts umfasst, wie die personale Selbstbestimmung (EGMR 2010: 53), das Sozialleben (EGMR 2018: 153) und das Recht am eigenen Bild (EGMR 2004: 50). Obwohl der EuGH bisher nur punktuell diese Rechte für Art. 7 GRCh anerkannt hat (vgl. Augsberg $^{7}$2015: 3), wird man darin jedoch genügenden Nachweis dafür sehen können, dass die Idee eines allgemeinen Persönlichkeitsrechts und einer darauf rekurrierenden informationellen Selbstbestimmung auch dem Art. 8 Abs. 1 GRCh nicht fremd ist.

Klement geht in seiner Herleitung einer informationellen Selbstbestimmung einen anderen Weg. Parallel zum Menschenwürdebezug im allgemeinen Persönlichkeitsrecht des Grundgesetzes ergebe sich auch aus der Achtung der Menschenwürde in Art. 1 Abs. 1 und Abs. 2 S. 1 der Präambel der EU-Grundrechtecharta eine »Respektierung des aus der Fähigkeit des Menschen zum Selbstentwurf resultierenden Achtungsanspruchs« (Klement 2017: 169). Im Zusammenspiel mit dem Schutz der Privatsphäre in Art. 7 GRCh sei eine »Mindestbedingung der Persönlichkeitsentfaltung« gegeben, die für die Möglichkeit des Selbstentwurfs aber die Interaktion mit anderen Grundrechtsträgern brauche. Eine freie Entfaltung der Persönlichkeit könne Art. 7 GRCh zwar nicht gewähren, jedoch »kann dem Grundrechtsträger das Recht darauf zugesprochen werden, selbst zu bestimmen, mit welchen Inhalten und in welchen Beziehungen er in den Prozess der interaktiven Persönlichkeitsentfaltung mit seiner Umwelt eintritt« (ebd.). Die informationelle Selbstbestimmung sei dann eine Ausprägung dieses Rechts auf interaktive Persönlichkeitsentfaltung. Dass der Art. 8 GRCh eigenständig sei, solle über die hergestellten Sinnbezüge auch dogmatisch erfasst werden (ebd.).

Die Herleitung eines eigenen auf Art. 7 und Art. 1 GRCh gestützten allgemeinen Persönlichkeitsrechts und einer daraus abgeleiteten informationellen Selbstbestimmung ließe sich selbstverständlich auch ohne die Existenz von Art. 8 GRCh erreichen. Der Bezug zu diesem bleibt unklar und auch wenn die informationelle Selbstbestimmung das Datenschutzgrundrecht mit umfasst, hängt Art. 8 GRCh doch eher annexartig an dieser Konzeption.

Ein weiteres, nicht gelöstes Problem liegt darin, dass beide Ansichten den Ausgangspunkt ihres allgemeinen Persönlichkeitsrechts im Schutz der Privatheit nehmen müssen, weil sowohl der EMRK als auch der GRCh ein dem Art. 2 Abs. 1 GG entsprechendes Recht auf freie Entfaltung der Persönlichkeit fehlen. Dennoch wird man im Ergebnis nicht sagen können, das Datenschutzgrundrecht des Art. 8 GRCh sei rein privatnützig, genauso wenig wie die informationelle Selbstbestimmung die Interessen der Allgemeinheit in den Fokus stellt, aber dennoch dürfte der Weg zu einer Begründung des Schutzes der Privatsphäre aus Sicht des EU-Datenschutzgrundrechtes kürzer sein und sich auf der Gegenseite eine in den Sozialraum gerichtete Sichtweise leichter begründen lässt, wenn man das Grundgesetz bemüht.

## 4. Exkurs: Art. 12a Hessische Verfassung – informationelle Selbstbestimmung in Reinform

Um einen vollständigen Blick über die Verfassungsfragen zum Datenschutz zu bekommen, muss man auch einen Blick in die Landesverfassungen der deutschen Bundesländer werfen. Aus der hessischen Perspektive dieses Beitrags ist das Art. 12 a der Hessischen Landesverfassung, mit welchem im Jahr 2018 in den Volksabstimmungen über die Änderung der Hessischen Landesverfassung ein Recht auf informationelle Selbstbestimmung bei 90,9-prozentiger Zustimmung mit folgendem Wortlaut angenommen wurde:

»Jeder Mensch ist berechtigt, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen. Die Vertraulichkeit und Integrität informationstechnischer Systeme werden gewährleistet. Einschränkungen dieser Rechte bedürfen eines Gesetzes.«

Der Wortlaut von Satz 1 entspricht dem Kern des durch das Volkszählungsurteil geschaffenen Rechts auf informationelle Selbstbestimmung aus Art. 2 I GG i.V.m. Art. 1 I GG. Satz 2 setzt das ebenfalls durch das BVerfG aus dem allgemeinen Persönlichkeitsrecht gebildete Recht auf Integrität informationstechnischer Systeme fest.

Selbstverständlich ist die Bedeutung eines Landesverfassungsgrundrechts begrenzt, wobei die eigenständige Geltung der Verfassung unter den Voraussetzungen des Art. 28 Abs. 1 GG garantiert ist (vgl. Schwarz 2018: 18). Eine Geltung für Landesbehörden kann ebenso angenommen werden wie eine Ausstrahlungswirkung auf die Rechtsordnungen anderer Bundesländer, von denen bisher zehn ein solches Recht auf informationelle Selbstbestimmung oder ein Datenschutzgrundrecht aufgenommen haben.

Inhaltlich gilt für Art. 12a HV das für die informationelle Selbstbestimmung Gesagte, wobei hier insbesondere in der Übernahme des Wortlauts des Volkszählungsurteils davon auszugehen ist, dass es sich um eine Konstruktion auf Basis des allgemeinen Persönlichkeitsrechts handelt (vgl. LT-Drs. 19/6376: 107). Somit ist auch hier eine Konzeption der informationellen Selbstbestimmung, in der die besondere Bedeutung der Datenverarbeitung für die Gesellschaft ohne großen Aufwand mitgedacht werden kann, herauszulesen.

## 5. Datensouveränität als Verantwortung

Auf den ersten Blick scheinen die Unterschiede zwischen der informationellen Selbstbestimmung des Grundgesetzes und dem EU-Datenschutzgrundrecht vernachlässigbar. Im Ergebnis sind die Schutzgüter und Gewährleistungen des deutschen und des europäischen Rechts auch weitgehend deckungsgleich. Dieser Beitrag hat dennoch aufgezeigt, dass Unterschiede bestehen und diese den Begründungsaufwand in die eine wie die andere Richtung beeinflussen. Wenn das EU-Datenschutzgrundrecht einen Fokus auf den Schutz der Privatsphäre zulässt, der in eine wegen ihrer Ökonomisierungsaspekte ebenfalls zu Recht kritisierte eigentumsähnliche Situation führt, macht es das dem Einzelnen vielleicht zu leicht, sich mit der gesellschaftlichen Bedeutung seiner Daten nicht auseinanderzusetzen. Dahingegen kann eine informationelle Selbstbestimmung, die von der Verhaltensfreiheit in der Beziehung zur Gesellschaft ausgeht, Daten in ihrer Funktion als »soziale Ressource« (Deutscher Ethikrat 2018: 253) besser in ein Konzept integrieren. Eine auf diesen Grundgedanken fußende Datensouveränität muss also nicht nur ein hohes Schutzniveau sicherstellen, sondern kann und soll den Einzelnen einfacher in die Lage versetzen, Verantwortung für den gesellschaftlichen Nutzen seiner Daten zu übernehmen. Dies beinhaltet den sicherlich Überwindung kostenden Schritt, die Tendenzen zu einer Verabsolutierung der Privatsphäre im bestehenden Datenschutzrecht zu überdenken, der auch immer mit der Furcht vor einem Absenken des Schutzniveaus verbunden ist. Am ehesten gelingen wird dies, wenn man den Datenschutz weniger von einem Standpunkt aus betrachtet, der auf den Schutz der Privatheit ausgerichtet ist, als vielmehr von einem, der auf der Verhaltensfreiheit fußt. So würde dann auch die gesellschaftliche Bedeutung der Datenverarbeitung von vorneherein mit in den Blick genommen werden.

# Datenschutz und Datensouveränität – ein Widerspruch?

*Anne Riechert*

## Einleitung

Die interdisziplinäre Diskussion über »Digitale Souveränität«, »Datensouveränität« und die grundsätzliche Frage, was »souverän« umfasst, hat die Vielschichtigkeit und Mehrdeutigkeit dieser Begriffe deutlich gezeigt. Es scheint nahezu unmöglich, eine einheitliche, übergreifende Definition der Datensouveränität zu finden, die alle Fachrichtungen gleichermaßen abdeckt. Der nachfolgende Beitrag widmet sich der Frage, ob es eines Begriffs wie »Datensouveränität« aus datenschutzrechtlicher Sicht überhaupt bedarf, gibt es doch vielfältige gesetzlich verankerte Instrumente, die dem Einzelnen als »Ausfluss« des gemäß Art. 2 Abs. 1 GG, Art. 1 Abs. 1 GG bestehenden informationellen Selbstbestimmungsrechts zur Verfügung stehen. Personenbezogene Daten einer natürlichen, der »betroffenen Person«, sind vor allem gemäß der Datenschutzgrundverordnung (DSGVO) geschützt. Fraglich ist daher gleichermaßen, ob ein Begriff der »Datensouveränität« sogar im Widerspruch zum »Schutz personenbezogener Daten« stehen könnte wie auch, ob er nicht in einer genauer zu klärenden Weise an die unternehmerische Freiheit als Paradigma anknüpft.[1]

Insbesondere können in diesem Zusammenhang wirtschaftliche und politische Interessen eine Rolle spielen. Dies ist namentlich im europäischen Kontext zu betrachten. Der Europäische Rat ruft etwa dazu auf, »das Potenzial von Daten und digitalen Technologien zum Vorteil der Gesellschaft, der Umwelt und der Wirtschaft besser zu nutzen, wobei die entsprechen-

1 Petra Gehring hat in ihrem Beitrag in diesem Band zudem begründet, dass »digitale Souveränität« und »Datensouveränität« zwei unterschiedliche Konzepte darstellen, was in zukünftigen Debatten zu berücksichtigen wäre.

den Rechte in Bezug auf den Datenschutz und die Privatsphäre sowie andere Grundrechte zu wahren sind« (Europäischer Rat 2021a: 4). Die Portabilität von Daten und die Interoperabilität von Diensten nehmen für diese Nutzbarkeit einen hohen Stellenwert ein und haben sowohl eine rechtliche als auch eine technische Relevanz. In diesem Sinne betont der Europäische Rat ebenso die Notwendigkeit, »qualitativ hochwertige Daten leichter verfügbar zu machen und eine bessere gemeinsame Nutzung und Zusammenführung von Daten sowie die Interoperabilität zu fördern und zu ermöglichen.« (Europäischer Rat 2020: 5) In seinen Erklärungen geht er ebenso auf die »Digitale Souveränität« ein (Europäischer Rat 2020: 3 f.; 2021a: 3).

## Datenschutz versus Datensouveränität?

### 1. Einwilligung

Sofern nur überhaupt Informationen verarbeitet werden, die sich auf eine natürliche Person beziehen, drängt sich auf den ersten Blick und unter Berücksichtigung des allgemeinen Sprachgebrauchs das Instrument der Einwilligung gemäß Art. 6 Abs. 1 lit a Datenschutzgrundverordnung (DSGVO) i.V.m. Art. 7 DSGVO für eine »souveräne« Datenverarbeitung geradezu auf.

Das Instrument und Format der Einwilligung verankert in der DSGVO einfachgesetzlich das durch Art. 8 Abs. 1 Grundrechte-Charta (GRCh) gewährleistete Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten, die gemäß Art. 8 Abs. 2 GRCh nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden dürfen (Taeger 2022: Art. 7 DSGVO Rn. 1.). Damit wird ebenso das informationelle Selbstbestimmungsrecht gemäß Art. 2 Abs. 1, Art. 1 Abs. 1 GG zum Ausdruck gebracht (ebd.).

Betroffene können einwilligen oder die Nutzung von Daten durch Verweigerung der Einwilligung verhindern. Sie wirken mit. Bedarf es daher in diesem Kontext überhaupt der Verwendung des Begriffs »Datensouveränität«? Diesbezüglich sind die Voraussetzungen der Einwilligung und die aktuelle Rechtspraxis in den Blick zu nehmen. Wichtig sind also sowohl Kontexte entstehender Normanwendung als auch Interpretationen dessen, was gesetzlicher Datenschutz am Ende des Tages wollen kann.

### a. *Zugriff auf Informationen in Endeinrichtungen*

In umschriebenen Problemzusammenhang ist das in Deutschland am 01.12.2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz zu beachten (TTDSG 2021), welches in § 25 TTDSG regelt, dass die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur als zulässig betrachtet werden können, wenn der Endnutzer[2] auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Vom Begriff der Endeinrichtung können Smart-Home-Geräte, vernetzte Kameras, etc. umfasst sein.[3] Die Einwilligung hat gemäß der DSGVO zu erfolgen, wobei Artikel 4 Nr. 11 DSGVO eine Einwilligung beschreibt als

> »jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung (…), mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist« (DSGVO 2016).

Was unter einer »eindeutig bestätigenden Handlung« zu verstehen ist, erläutert Erwägungsgrund 32 S. 2 DSGVO: Eine solche Handlung kann durch das Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen

2 Gemäß § 2 Abs. 1 TTDSG gelten für den Begriff des Endnutzers die Begriffsbestimmungen des TKG. Der Begriff des »Endnutzers« ist nun in § 3 Nr. 13 TKG geregelt und entspricht dem bisherigen § 3 Nr. 8 TKG a. F. Gemäß § 3 Nr. 13 TKG ist »Endnutzer« ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt. Die Aufsichtsbehörden verweisen darauf, dass der Begriff des Endnutzers im Telekommunikationsrecht vor allem der Abgrenzung zu Anbieter:innen von Telekommunikationsdiensten diene, nicht aber zur Spezifizierung oder gar Eingrenzung des persönlichen Anwendungsbereichs von § 25 TTDSG (OH Telemedien 2021: 10 f.).

3 Nach § 2 Abs. 2 Nr. 6 TTDSG ist eine »Endeinrichtung« jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten. Siehe zur Begriffsdefinition auch Schumacher/Sydow/von Schönfeld 2021: 603 f.

Kontext eindeutig ihr Einverständnis mit der beabsichtigten Datenverarbeitung signalisiert.[4]

Einer eigenständigen Interpretation der Einwilligungsvoraussetzungen durch die Unternehmen, gerade mit Blick auf Erwägungsgrund 32 S. 2 DSGVO, der auf ein »signalisiertes« Einverständnis der Betroffenen verweist, schieben jedoch die Datenschutzbehörden einen Riegel vor. So stellt die reine weitere Nutzung einer Webseite oder App, z. B. durch Handlungen wie das Herunterscrollen, das Surfen durch Webseiteninhalte, das Anklicken von Inhalten oder ähnliche Aktionen keine wirksame Einwilligung dar (OH Telemedien 2021: 12).[5] Der Schutz der Betroffenen wird daher in diesem Kontext, man »scrollt« nun einmal ohne viel zu wissen oder zu wollen, den Realitäten angepasst. Vor allem aber wird das gewiss zu Recht von den Beteiligten erwartete Schutzniveau durch Leitlinien der Aufsichtsbehörden und nicht durch eine – wie auch immer ausgeformte – Begriffsdefinition sichergestellt.

Die Vorschrift des § 25 TTDSG bestätigt außerdem nur die bereits bestehende Rechtslage zum Datenschutz. Es wird die Vereinbarkeit konkreter Bestimmungen mit höherrangigem Recht hergestellt.[6] Denn § 25 TTDSG bezieht sich auf den Wortlaut von Art. 5 Abs. 3 der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) und stellt klar, dass der Endnutzer davor geschützt ist, dass Dritte unbefugt auf seiner Endeinrichtung Informationen speichern oder auslesen und dadurch seine Privatsphäre verletzen.[7] Cookies dürfen daher nicht bereits mit dem erstmaligen Aufruf einer Webseite gesetzt werden, sondern zuvor ist die Einwilligung einzuholen.[8] Dieses Erfordernis dient der Rechtssicherheit. Im Gegensatz dazu hatte § 15 Abs. 3 S. 1 TMG

4 Plath 2018, Art. 7 DSGVO Rn. 11 verweist auf das »Häkchensetzen« als Hauptanwendungsfall in der Wirtschaft. Siehe zur aktiven Handlung auch Der Bayerische Landesbeauftragte für den Datenschutz 2021: Rn. 58 ff.

5 Siehe auch Buchner/Kühling 2020: Art. 7 DSGVO Rn. 58 c.

6 Siehe zur verzögerten Umsetzung von Art. 5 Abs. 3 ePrivacy-Richtlinie auch Jandt 2021: 66 f.

7 Siehe hierzu auch den Gesetzentwurf der Bundesregierung vom 10.02.2021 (Bundesregierung 2021b: 41).

8 Siehe zum Zeitpunkt der Einwilligung Arning/Rothkegel 2022: Art. 4 Nr. 11 DSGVO Rn. 360; OH Telemedien 2021: 10 f. Siehe aber auch Der Bayerische Landesbeauftragte für den Datenschutz 2021: Rn. 61 mit dem Hinweis, dass dies zwar keine Vorgabe des Art. 4 Nr. 11 DSGVO sei, aber dem Grundsatz der Rechtmäßigkeit des Art. 6 DSGVO entspreche, dass eine wirksame Rechtsgrundlage für die fragliche Datenverarbeitung bereits zu Beginn gegeben sein müsse. Siehe hierzu außerdem Europäischer Datenschutzausschuss 2020: 23. Der Europäische Datenschutzausschuss verweist ferner darauf (S. 4), dass es sich bei dem vorliegenden Dokument um eine geringfügig aktualisierte Fassung der Leitlinien der Artikel-29-Datenschutzgruppe vom 10.04.2018 handelt,

a.F. eine Widerspruchslösung für das Setzen von Cookies vorgesehen.[9] Zu beachten ist, dass sich § 25 TTDSG auf alle Informationen bezieht, die ein Drittanbieter auf Geräten speichert oder abruft. Dies betrifft nicht nur sogenannte Cookies, sondern es kann ebenso das sogenannte Browser-Fingerprinting umfassen (Hanloser 2021: 399).[10] In diesem Sinne argumentieren die Aufsichtsbehörden gleichermaßen, dass ein technologieneutrales Verständnis im Rahmen der Auslegung zugrunde zu legen ist und außerdem Endnutzer bzw. Einwilligungsberechtigter derjenige ist, der objektiv die Endeinrichtung nutzt, wobei Eigentumsverhältnisse keine Rolle spielen sollen (OH Telemedien 2021: 11 und Der Bayerische Landesbeauftragte für den Datenschutz 2021: Rn. 26). Die Datenschutzbehörden, die für die Verhängung von Bußgeldern zuständig sind, nehmen daher auch hier eine korrigierende bzw. konkretisierende Auslegung des Wortlauts zum Schutz der Betroffenen vor. Selbst wenn jedoch eine andere Rechtsauffassung vertreten und *ebenso Unternehmen* im Einzelfall als einwilligungsberechtigt betrachtet werden sollten, bedarf es in diesem Zusammenhang nicht zwangsläufig einer zusätzlichen Begriffsbildung wie »Datensouveränität«, sondern vielmehr einer anderen Begriffsdefinition des »einwilligungsberechtigten Endnutzers«. Ein Instrument zur Stärkung von Betroffenenrechten besitzt das geltende Recht bereits.

---

die vom Europäischen Datenschutzausschuss (im Folgenden »EDSA«) in seiner ersten Plenumssitzung gebilligt wurden.

9 Der EuGH entschied – nach einer Vorlage zur Vorabentscheidung durch den BGH – mit Urteil vom 01.10.2019, dass es sich nicht um eine wirksame Einwilligung i. S. d. Art. 6 Abs. 1 lit. a DSGVO handelt, »wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss«. Der EuGH begründete, dass Art. 2 lit. f und Art. 5 Abs. 3 ePrivacy-Richtlinie dahin auszulegen sind, dass in diesem Falle keine wirksame Einwilligung im Sinne dieser Bestimmungen vorliegt. Dies wird nun in § 25 TTDSG entsprechend umgesetzt. Die weitere Datenverarbeitung richtet sich wiederum nach den Regelungen der DSGVO. Siehe zum Vorabentscheidungsersuchen: BGH MMR 2018: 90; BGH ZD 2018: 79 mit Anmerkung Ettig/Rauer. Siehe außerdem Ogorek 2020: 478, 480. Siehe insgesamt EuGH, Urteil vom 01.10.2019 – C-673/17; EuGH MMR 2019: 732 ff.; EuGH GRUR 2019: 1198 ff.; EuGH ZD 2019: 556 ff. mit Anmerkung Hanloser.

10 Hanloser verweist darauf, dass dies eine Vorschrift zum Schutz von »Informationen auf Endgeräten« sei, die sich nicht nur auf Cookies, sondern letztlich auf alle Informationen beziehe, die ein Drittanbieter auf Geräten ablegt oder abruft, die mit öffentlichen Telekommunikationsnetzen (insbesondere mit dem Internet) verbunden sind. Siehe zu »cookielosen Trackingansätzen« außerdem Scharpf 2021: 379 ff., insbesondere 385 f.

Die Frage von »Datensouveränität« könnte darüber hinaus mit Blick auf »berechtigte Interessen« diskutiert werden. So kann sich die anschließende Datenverarbeitung im Rahmen der Einwilligung von § 25 TTDSG auf »berechtigte Interessen« des Verantwortlichen gemäß Art. 6 Abs. 1 lit. f DSGVO stützen.[11] Art. 6 Abs. 1 lit. f DSGVO ist eine Rechtsgrundlage, die in der Praxis oftmals sowohl weit ausgelegt als auch in Datenschutzrichtlinien gemeinsam mit anderen Rechtsgrundlagen zur Datenverarbeitung angegeben wird,[12] obwohl nach Auffassung der Aufsichtsbehörden die Verantwortlichen *vor* der Erhebung zu entscheiden haben, welche Rechtsgrundlage zur Anwendung gelangt (Europäischer Datenschutzausschuss 2020: 30). Fraglich könnte zwar sein, ob mit der Regelung von »berechtigten Interessen« im Gesamten eine gesetzgeberische Entscheidung für »Datensouveränität von Unternehmen« auf der Grundlage von unternehmerischer Freiheit i.S.v. Artikel 16 GRCh verbunden sein könnte. Es erscheint dennoch weder erforderlich noch geboten, die Datenverarbeitung aufgrund »berechtigter Interessen« außerhalb eines datenschutzrechtlichen Kontextes zu betrachten, da stets eine Abwägung mit den Grundrechten und Grundfreiheiten betroffener Personen erfolgen muss. Dafür bedarf es ebenfalls keines zusätzlichen Begriffs wie »Datensouveränität«, wenn man ihn als Gegenpart zum Grundrecht auf Datenschutz versteht. Entsprechende Überlegungen gelten in analoger Weise für den aktuellen Entwurf des Ministerrates zur ePrivacy-Verordnung vom 10.02.2021, der Verarbeitungsmöglichkeiten für »kompatible Zwecke« vorsieht (Europäischer Rat 2021b: 6087/21),[13] aber

---

11 § 25 TTDSG bezieht sich ausschließlich auf die in der Endeinrichtung gespeicherten oder ausgelesenen Daten. Vgl. OH Telemedien 2021: 27 ff., Hanloser, 2021: 399 f. Siehe zur strengen Zweckbindung des TTDSG darüber hinaus Hanloser 2021: 399, 402.

12 Ein Beispiel ist der Dienst »Spotify«, der in seinen Datenschutzrichtlinien mehrere Rechtsgrundlagen für einen Verarbeitungszweck angibt, etwa die Verarbeitung von Nutzerdaten und Nutzungsdaten auf der Grundlage von »berechtigen Interessen« neben der »Erforderlichkeit zur Vertragserfüllung«, »um Probleme mit dem Spotify Service zu verstehen, zu diagnostizieren und zu beheben«, abrufbar unter: www.spotify.com/de/legal/privacy-policy/#04-zweck-unserer-nutzung-ihrer-personenbezogenen-daten. Zur Frage und Auslegung von »berechtigten Interessen« siehe Artikel-29-Datenschutzgruppe 2014.

13 Dieses Dokument des EU-Ministerrates liegt den Trilog-Verhandlungen mit dem Europäischen Parlament zugrunde. Eine Verarbeitungsmöglichkeit für kompatible Zwecke war im ersten Entwurf der EU-Kommission zur ePrivacy-Verordnung vom 10.01.2017 nicht enthalten (Europäisches Parlament 2017).

insgesamt Regelungen zum Datenschutz und zum Schutz der Privatsphäre enthält.[14]

Es fragt sich also: Wo besteht daher insgesamt noch Schutzbedarf für die Betroffenen oder gar Bedarf an einer darüberhinausgehenden »Datensouveränität« und welchen Inhalt sowie Zweck könnte der Begriff »Datensouveränität« in diesem Kontext erfüllen?

### *b. Automatisierte Entscheidung*

Tatsächlich reicht die Betrachtung des Grundrechts allein nicht aus. Denn in der Praxis gerät im digitalen Alltag die Einwilligung an ihre Grenzen. Es wird stets auf die »Banner-Flut« hingewiesen (Golland 2021: 3 ff.).[15] Und jeder kennt das Phänomen des schnellen Weg-Klickens absichtsvoll kompliziert gestalteter Privacy-Voreinstellungen. Ist die Einwilligung daher einerseits das klassische Instrument, um informationelle Selbstbestimmung sicherzustellen, ist diese andererseits in Zeiten der (unüberschaubaren) Vernetzung, Digitalisierung und dem Einsatz von Künstlicher Intelligenz nunmehr mit Zweifeln behaftet. Welcher Nutzer, welche Nutzerin ist in der Lage, die Datenverarbeitung in ihrer Komplexität tatsächlich zu erfassen und selbstbestimmt einzuwilligen?

Der Sachverständigenrat für Verbraucherfragen weist in einer Marktstudie darauf hin, dass in immer mehr Lebensbereichen mit immer komplexeren Verfahren Eigenschaften und Aktivitäten von VerbraucherInnen analysiert werden, und zwar im Sinne von Prognosen über ihr künftiges Verhalten (Sachverständigenrat für Verbraucherfragen 2018: 14). Dies bedeutet, dass eine formalisierte Einschätzung von Personen mit Hilfe einer Zahl (Scoring) vorgenommen wird, was unterschiedliche Branchen betreffen kann (Finanzbranche, Versicherungsbranche) (Sachverständigenrat für Verbraucherfragen 2018: 14). Längst hängen viele reale Marktkonditionen davon ab, dass wir uns »angepasst« verhalten. Aber gehört nicht auch zu unserer »souveränen« Lebensgestaltung, selbstständig zu entscheiden, sich solchen Regelungen zu unterwerfen, die die Tarifgestaltung davon abhängig machen, wie oft ich

14 Die Fassung der ePrivacy-Verordnung vom 10.01.2017 bildete außerdem zu dem damaligen Zeitpunkt noch eine Herangehensweise ab, die vom Europäischen Datenschutzausschuss unterstützt wurde: »breite Verbote, enge Ausnahmen und die Einwilligung in die Verarbeitung der Daten« (Europäischer Datenschutzausschusses 2020). Siehe außerdem: Europäischer Datenschutzausschuss 2018.

15 Golland weist auf eine »Einwilligeritis« hin.

beim Autofahren bremse oder ob ich rauche und mich ausreichend körperlich bewege? Problematisch ist allerdings, wenn die zugrunde liegenden algorithmischen Entscheidungsverfahren falsche Bewertungen der Personen enthalten und sich Bewertungsmuster verfestigen. Künstlicher Intelligenz liegen Algorithmen zugrunde, die solche Bewertungsmuster automatisiert und lernend erstellen. Die Datenethikkommission definiert Künstliche Intelligenz insgesamt

»als Sammelbegriff für diejenigen Technologien und ihre Anwendungen, die durch digitale Methoden auf der Grundlage potenziell sehr großer und heterogener Datensätze in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess ein Ergebnis ermitteln, das ggf. automatisiert zur Anwendung gebracht wird« (Datenethikkommission 2019: 34).

Daran anknüpfend fordert die Datenethikkommission, dass Künstliche Intelligenz »keine tendenziöse Vorfestlegungen« und »keine systematische Verzerrungen« enthalten dürfe, sogenannte Biases (Datenethikkommission 2019: 167). Auch ohne eine allgemein anerkannte Definition für KI lassen sich datenschutzrechtliche Herausforderungen benennen, die mit ihr verbunden sind. So hat die Datenschutzkonferenz in ihrer so genannten »Hambacher Erklärung« sieben datenschutzrechtliche Anforderungen für Künstliche Intelligenz aufgestellt, unter anderem, dass KI nachvollziehbar, transparent und erklärbar sein muss, Verantwortlichkeit und eine sichere Datenverarbeitung braucht, und der Mensch nicht zum Objekt werden darf (Datenschutzkonferenz 2019).

Aufgegriffen wird die zuletzt genannte Anforderung durch den Vorschlag zu einer KI-Verordnung, die gemäß Artikel 14 eine menschliche Aufsicht für Hochrisiko-KI-Systeme verlangt (Europäisches Parlament 2021). Außerdem regelt Artikel 22 DSGVO, dass die betroffene Person das Recht hat, nicht einer *ausschließlich* auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[16] Das Verbot einer »ausschließlich auto-

16 Ausnahmen von diesem grundsätzlichen Verbot ergeben sich jedoch im Falle der ausdrücklichen Einwilligung der betroffenen Personen oder wenn die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (Art. 22 Abs. 2 DSGVO).

matisierten Entscheidung« bedeutet, dass das Recht hier ein menschliches Korrektiv bzw. Überprüfung durch einen Menschen verlangt.[17]

Man könnte meinen, diese menschliche Intervention gehe über die eigentlichen Datenschutzinteressen hinaus, da die automatisierte Bewertung und nicht die Bewertung an sich im Mittelpunkt der Betrachtung steht. Allein die Tatsache, dass nicht ein Mensch, sondern eine Maschine entscheidet, hat den Gesetzgeber bereits in § 6a BDSG a.F. dazu bewogen, dies im Rahmen von datenschutzrechtlichen Bestimmungen zu verankern, obwohl eher eine Nähe zum Persönlichkeitsschutz, zu unserer Privatsphäre, besteht, verbunden mit der gesetzgeberischen Wertung, dass wir einer Maschine grundsätzlich nicht trauen können und wir daher geschützt werden müssen.[18]

Der konkrete Bezug zum Schutz der personenbezogenen Daten erfolgt allerdings dadurch, dass diese automatisierte Bewertung auf Daten beruht und dieser schon rein technisch stets ein Muster inhärent ist, welches sich festsetzen kann, schwer revidierbar ist und regelmäßig Informationen betrifft, aus denen sich wiederum Schlussfolgerungen über das Privatleben ziehen lassen, z. B. in Bezug auf ihre Gewohnheiten im Alltag, Interessen oder (vermeintliche) Charaktereigenschaften. Dieses Muster im Sinne einer Profilbildung kann angewendet werden, um zu entscheiden, ob wir einen Rabatt oder einen Kredit erhalten, ob wir suizidgefährdet sind oder welcher Partner am besten zu uns passt. Die zugrunde liegende Datenbasis stellt hierfür einen wichtigen Faktor dar. Im Vorschlag einer KI-Verordnung für »Hochrisiko-KI-Systeme« wird in diesem Sinne geregelt, dass »Trainings-, Validierungs- und Testdatensätze« u. a. »relevant, repräsentativ, fehlerfrei und vollständig« sein müssen (Art. 10 Abs. 3 S. 1 des Entwurfs einer KI-Verordnung).[19]

---

17 Siehe Buchner 2020: Art. 22 DSGVO Rn. 15 zur inhaltlichen Mitverantwortung der Entscheidung durch einen Menschen.

18 Zu berücksichtigen ist ebenso, dass von Artikel 22 DSGVO die Profilbildung als solche nicht erfasst ist. Grundsätzlich kann diese gemäß Art. 6 Abs. 1 lit. f DSGVO auf berechtigten Interessen des Unternehmens beruhen, welches die Profilbildung vornimmt. Art. 6 Abs. 1 lit. f DSGVO regelt, dass die Datenverarbeitung rechtmäßig ist, wenn »die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich« ist, »sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt«.

19 Diese Datensätze müssen gemäß Art. 10 Abs. 3 S. 2 des Entwurfs der KI-Verordnung der EU außerdem »die geeigneten statistischen Merkmale« haben, »gegebenenfalls auch bezüglich der

Hinsichtlich der Frage, wo in diesem Rahmen ein Bezug zur »Datensouveränität« bestehen könnte, sind die Gutachten des Rats für Digitale Ökologie sowie des Sachverständigenrats für Verbraucherfragen anzuführen, die sich auf u. a. Bildungsfragen beziehen. So weist der Rat für Digitale Ökologie darauf hin, »dass die Gesellschaft undurchschaubarer wird, da algorithmische Prozesse nicht von außen einsehbar sind« (Rat für Digitale Ökologie 2021). »Ein technisches Verständnis der Digitalen Transformation« sei

> »deshalb für die Erlangung digitaler Souveränität unabdingbar. Der Sachverständigenrat für Verbraucherfragen hebt hervor, dass Verbraucher in der Lage sein sollten, ihren Bedarf an Informationen überhaupt zu bestimmen, Informationen zu finden, hinsichtlich ihrer Relevanz, Qualität, Reichweite und Aussagekraft zu beurteilen und zu bewerten, Informationen für sich zu verarbeiten und neu aufzubereiten und ggf. auch anderen zugänglich zu machen.« (Sachverständigenrat für Verbraucherfragen 2017)

Die datenschutzrechtlichen Regelungen zur Einwilligung sind daher nicht ausreichend, um den Schutzbedarf der Betroffenen auch zukünftig in der Praxis sicherzustellen, sondern es wird ein darüberhinausgehender Bedarf an digitaler Bildung angemeldet, um eine immer komplexer werdende Materie zu begreifen. Diese Kompetenz, die das Individuum braucht, wird von den AutorInnen der gerade genannten Gutachten nun tatsächlich als »Digitale Souveränität« umschrieben, und die Forderung nach dieser Souveränität kann als staatlicher Regelungsauftrag verstanden werden.[20] Allerdings sollte ebenso berücksichtigt werden, dass Bildung zwar eine wichtige Forderung darstellt, jedoch allein nicht ausreichend erscheint, um die Komplexität der Datenverarbeitung in den Griff zu bekommen oder um den Begriff der »Datensouveränität« umfassend abzubilden. Im Einzelfall können Betroffene ja trotzdem überfordert sein. Insbesondere wäre eine im allgemeinen Sprachgebrauch verwendete Begriffsbestimmung von »souverän« als »überlegen« nicht passend. Auch digital kompetente Betroffene sind bei komplexen, automatisierten Prozessen regelmäßig nicht in der Lage, eine einer Maschine überlegene Entscheidung zu treffen. Eventuell würden sie – gepaart mit ihren jeweiligen sozialen sowie menschlichen Fähigkeiten – allenfalls

Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll«. Hier stellt sich jedoch die praktische Frage, wie eine solche Datenbasis generiert werden soll.

20 Hieran zeigt sich auch wiederum die Wichtigkeit der Abgrenzung der Begrifflichkeiten von »Datensouveränität« und »Digitaler Souveränität«. Siehe hierzu den Beitrag von Gehring in diesem Band.

hier und da die bessere oder zumindest eine andere Entscheidung treffen als eine ungeschulte Person.

Somit sollte der Ausgangspunkt der rechtlichen Bewertung der mit den Bedingungen des Einwilligens aufgeworfenen Fragestellung nicht die individuelle Kompetenz sein. Vielmehr könnten Kontrollmechanismen, Zertifizierungen oder Gütesiegel dabei unterstützen, den Schutz der Betroffenen sicherzustellen und diesen gleichzeitig signalisieren, dass eine »geprüfte« Datenverarbeitung vorliegt. Die Datenethikkommission hat hier bereits über eine bloße Datenschutz-Folgenabschätzung hinausgehend eine Risikofolgenabschätzung für algorithmische Systeme gefordert (Datenethikkommission 2019: 188 ff.). Damit soll gerade auch Risiken außerhalb des Datenschutzes begegnet werden.

Ein derartiger Prüf-Mechanismus könnte insoweit mit dem Begriff der »Datensouveränität« verknüpft werden, als er über eine reine Kontrolle hinaus eine mitwirkende Teilhabe der Betroffenen sicherstellt, die ein Gestaltungsrecht umfasst.[21] In diesem Sinne könnte auch das notwendige Vertrauen geschaffen werden, Daten »preiszugeben«.

## 2. Einwilligungsverwaltung

Eine weitere Frage ist, ob neue Instrumente, wie die Einwilligungsverwaltung des § 26 TTDSG, die Betroffenen unterstützen oder gegebenenfalls auch einen »Mehrwert« schaffen, der über datenschutzrechtliche Aspekte hinausgeht.[22] Einwilligungsverwaltung – damit sind unter anderem die sogenannten PIMS, also softwaregestützte Managementsysteme für eine aktive Weitergabe der eigenen Daten gemeint. § 26 TTDSG bezieht sich ausschließlich auf die Einwilligungen des § 25 TTDSG, dementsprechend auf die Einwilligung in das Speichern oder Auslesen von Informationen, die auf Endeinrichtungen gespeichert sind, etwa Cookies (siehe oben). Die Bereitstellung und Verwaltung von personenbezogenen Daten, z. B. im Rahmen von Verbraucherverträgen (§ 312 BGB),[23] erfasst das Gesetz also

21 Siehe zum Begriff einer mitwirkenden Teilhabe von Bürgerinnen und Bürgern im Kontext des Dateneigentums: Fezer 2019: 148.

22 Zu den Anforderungen von § 26 TTDSG siehe auch Golland/Riechert 2022: § 26 TTDSG Rn. 5 ff.

23 Im Übrigen kommen aus datenschutzrechtlicher Sicht für die Bereitstellung der Daten unterschiedliche Rechtsgrundlagen in Betracht. Die Aufsichtsbehörden heben in diesem Zusammenhang hervor, dass eine der sechs Rechtsgrundlagen des Artikel 6 DSGVO vor der Verarbeitungstä-

nicht. Dies bedeutet aber auch, dass weder die Monetarisierung noch der freie Austausch von Daten, sondern doch wieder der klassische Datenschutz im Fokus stehen, und zwar die Ausübung von Kontrollmöglichkeiten über Informationen, die in dem Endgerät gespeichert werden oder auf die ein Zugriff erfolgen soll.[24] Für die Diskussion über Datensouveränität erscheint es also fraglich, ob § 26 TTDSG über den Schutz der personenbezogenen Daten hinaus die Rechtsposition von Dateninhaberinnen und Dateninhabern stärkt. Die Regelung ist allein auf den Schutz von Individualinteressen bzw. den Schutz der Betroffenen ausgerichtet.

Die von § 26 TTDSG umfassten Ziele sind zudem hinsichtlich ihrer praktischen Umsetzung mit erheblichen Zweifeln behaftet: Grundsätzlich muss im Rahmen der §§ 25, 26 TTDSG die betroffene Person ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke geben.[25] Diese enge Zweckbindung soll Kontrolle und Transparenz für die betroffene Person sicherstellen und ist eng mit dem Erfordernis der Einwilligung »in informierter Weise« verknüpft (Europäischer Datenschutzausschuss 2020). Es bedarf hierbei einer granularen Einwilligung, um das Merkmal einer Einwilligung für unterschiedliche Zwecke umzusetzen.[26] Pauschal- und Blankoeinwilligungen sind grundsätzlich unwirksam (Arning/Rothkegel 2022: Art. 4 Nr. 11 DSGVO Rn. 329). Ebenso sind generische, allgemeine oder vage Angaben grundsätzlich zu unbestimmt, etwa Aussagen wie »Verbesserung der Erfahrungen des Nut-

tigkeit und in Bezug auf einen spezifischen Zweck festgelegt werden müsse. Der Verantwortliche könne sich daher beispielsweise nicht rückwirkend auf das berechtigte Interesse als Grundlage für die Rechtfertigung der Verarbeitung berufen, wenn Probleme mit der Gültigkeit der Einwilligung aufgetreten sind (Europäischer Datenschutzausschuss 2020: 30). Unklar ist daher auch die rechtliche Situation beim Widerruf der Einwilligung, siehe hierzu Spindler 2021a: 528, 530 mit dem Hinweis, dass es umstritten sei, ob nach einem Widerruf der Einwilligung durch den Verbraucher ein Rückgriff auf andere Tatbestände des Artikel 6 DSGVO in Betracht kommt.

24 Botta 2021: 946 f. verweist darauf, dass sich der Bundesgesetzgeber gegen die Überlegung entschieden hat, dass Nutzer ihre Daten via PIMS monetarisieren können. Dennoch sei ein kommerzielles PIMS-Angebot nicht generell ausgeschlossen, da sich das Verbot wirtschaftlicher Eigeninteressen auf die Datenverwertung und nicht auf die Einwilligungsverwaltung als solche bezieht.

25 Zur Bestimmtheit der Einwilligung siehe auch Arning/Rothkegel 2022: Art. 4 DSGVO Rn. 325.

26 Siehe auch Arning/Rothkegel 2022: Art. 4 DSGVO Rn. 328; Buchner/Kühling 2020: Art. 4 Nr. 11 DSGVO Rn. 7 sowie Art. 6 DSGVO Rn. 179; Europäischer Datenschutzausschuss 2020: 17.

zers«, »Werbezwecke«, »IT-Sicherheitszwecke«, »zukünftige Forschung« oder »Verbesserung des Surferlebnisses«.[27]

Wenn zuvor granulare Voreinstellungen vorgenommen werden müssen, stellt sich die grundsätzliche Frage, worin überhaupt die Erleichterung der Einwilligungsverwaltung i. S. v. § 26 TTDSG liegt. Die dem Gesetz zugrunde liegende Denkweise erinnert vom Grundprinzip an das alte, inzwischen gar nicht mehr verwendete Protokoll P3P. Auch ist unklar, ob viele Schnittstellen zu unterschiedlichen Anbietern sich sogar nachteilig auf den eigentlich angestrebten Schutz der Privatsphäre auswirken könnten.[28] Rechtlich umstritten ist ebenso, ob eine Stellvertretung bei Erteilung und Widerruf von Einwilligungen möglich ist (Specht-Riemenschneider u. a. 2021: 25, 46). Näheres soll gemäß § 26 Abs. 2 TTDSG eine Rechtsverordnung regeln, die jedoch erst Ende 2022 zu erwarten sein dürfte. Ein entsprechendes Gutachten zum Einwilligungsmanagement nach § 26 TTDSG ist mittlerweile veröffentlicht (Stiemerling/Weiß/Wendehorst 2021: 45).

Ergänzend ist schließlich die europäische Rechtsentwicklung zu beachten: Ist hier auf dem Weg über die Einwilligungsverwaltung ein Mehr an Datensouveränität zu erwarten? Derzeit finden tatsächlich zum einen Trilogverhandlungen zur neuen ePrivacy-Verordnung statt, die Regelungen »über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG« enthält (siehe oben) (Europäisches Parlament 2017). Gemäß Art. 9 Abs. 2 dieses Vorschlags kann die Einwilligung auch mittels einer Software erteilt werden. Erwägungsgrund 22 verweist in diesem Zusammenhang darauf, dass »Webbrowser insbesondere als Torwächter dienen« und den Endnutzern helfen können, ein »Speichern von Informationen in ihren Endeinrichtungen (wie Smartphones, Tablets oder Computer) bzw. den Zugriff darauf zu verhindern«.

Zum anderen hat der neue Data Governance Act (DGA) der EU die verbesserte Handlungsfähigkeit und Kontrollmöglichkeiten des Einzelnen in Bezug auf die ihn betreffenden Daten im Fokus – insbesondere mit dessen Er-

---

27 Siehe zur »Verbesserung des Surferlebnisses« die Ausführungen von Der Bayerische Landesbeauftragte für den Datenschutz 2021: Rn. 67. Siehe zu vagen oder allgemeinen Angaben wie »Verbesserung der Erfahrungen des Nutzers«, »Werbezwecke«, »IT-Sicherheitszwecke« oder »zukünftige Forschung: OH Telemedien 2021: 14 mit Verweis auf die Stellungnahme von Artikel 29-Datenschutzgruppe 2013: 16.

28 Siehe zu Browsereinstellungen im Rahmen von § 26 TTDSG außerdem Die Landesbeauftragte für den Datenschutz Niedersachsen 2021: 2.

wägungsgründen 23, 25, 26 (Europäisches Parlament 2020). Art. 9 Abs. 1 lit. c DGA-Entwurf zählt beispielsweise Datengenossenschaften auf, die betroffene Personen bei der Ausübung ihrer Rechte an eigenen Daten unterstützen sollen.

Somit muss § 26 TTDSG letztendlich im europäischen Kontext ausgelegt werden, und die Regelung wäre bei Inkrafttreten der ePrivacy-Verordnung und des Data Governance Act obsolet oder müsste zumindest abgeändert werden. Daher ist § 26 TTDSG als Vorstufe oder »Zwischenlösung« einer europaweit geltenden Regelung zu betrachten (Schwartmann/Benedikt/Reif 2021: 99, 101).[29] Diese europäische Lösung, wie sie auch der Data Governance Act vorsieht, würde mit den entsprechenden Vorschlägen zu Datengenossenschaften oder »Datenaltruismus« über den Ansatz der DSGVO hinausgehen. Zwar will der DGA die Bestimmungen der DSGVO nicht berühren (siehe Erwägungsgrund 3 des DGA). Jedoch ist die europarechtliche Entwicklung ein entscheidender Faktor für eine Neugestaltung. Dies ist Gegenstand des nachfolgenden Abschnitts.

## 3. Datenaustausch – Datenteilung

Der Sachverständigenrat für Verbraucherfragen empfiehlt die Entwicklung eines verbraucherzentrierten Datenportals (Dashboard) zur Realisierung der individuellen Datensouveränität (Sachverständigenrat für Verbraucherfragen 2017: 8). Die Verbraucherzentrale Bundesverband e.V. nimmt auf technische Ansätze Bezug, mit deren Hilfe Endnutzer die Speicherung von Informationen in ihren Endeinrichtungen oder den Zugriff auf solche Informationen zentral steuern können. Dies soll auch ein Whitelisting umfassen, das »möglichst einfach« durch die entsprechende Software erfolgen soll, wenn dem Anbieter eines Dienstes eine Einwilligung zur Speicherung von Informationen auf dem Endgerät erteilt wurde (Verbraucherzentrale Bundesverband e.V. 2021: 5).[30] Dies steht ebenfalls im Zusammenhang mit den sogenannten »PIMS«. Die Datenethikkommission hat sich in

29 Mit dem Hinweis, dass »nur eine einheitliche europäische PIMS-Regelung Sinn« macht und sich der deutsche Gesetzgeber am Entwurf des Art. 11 Data Governance Act orientieren sollte. Ebenso Verbraucherzentrale Bundesverband e.V. 2021: 4 mit dem Hinweis, dass entsprechende Vorgaben auf EU-Ebene verankert werden sollten.

30 Siehe auch Verbraucherzentrale Bundesverband e.V. 2020: 6: »Kerngedanke dieses Konzeptes ist, den einzelnen Verbraucher in das Zentrum des Datenmanagements zu stellen.«

ihrem Abschlussbericht allgemein für die Entwicklung innovativer Einwilligungsmodelle, wie z. B. PIMS, im Forschungskontext ausgesprochen (Datenethikkommission 2019: 126). In der Praxis wird dabei einerseits auf unterschiedliche Kategorien, wie u. a. »Datenschutz-Assistenten, Einwilligungsmanagement-Systeme, Daten-Cockpits« verwiesen (Fokusgruppe Datenschutz 2020: 11 f.), oder es werden Datentreuhänder genannt (Fokusgruppe Datenschutz 2020: 13).[31] Andererseits werden Begriffe wie »Personal Management Tools (PMT)« oder »Datenagenten« von PIMS aber auch abgegrenzt. In letzterem Sinne wird begründet, dass bei »PMT« die Bereitstellung einer technischen Applikation im Vordergrund« stehe, bei PIMS die inhaltliche Dienstleistung, während Datenagenten nach den Vorgaben des Betroffenen automatisierte Entscheidungen treffen würden (Specht-Riemenschneider u. a. 2021: 25, 27).

Insgesamt handelt es sich bei PIMS »um neue Technologien und Ökosysteme, mit denen Menschen in die Lage versetzt werden sollen, über die Erhebung und Weitergabe ihrer personenbezogenen Daten Kontrolle auszuüben.« (Verbraucherzentrale Bundesverband e.V. 2020: 6) Der Europäische Datenschutzbeauftragte hebt den »am Menschen orientierten Ansatz in Bezug auf personenbezogene Informationen« hervor (Europäischer Datenschutzbeauftragter 2020). Der Einsatz der Systeme kann über die Einwilligungsverwaltung des § 26 TTDSG und auch über Kontrollrechte hinausgehen, insoweit könnte er den Begriff der »Datensouveränität« durchaus ausfüllen, zumal mit dem Einwilligen oftmals gleichzeitig ein (gegebenenfalls zweckgebundenes) Teilen von Daten verbunden ist.[32]

31 Siehe darüber hinaus die Hinweise von Specht-Riemenschneider u. a. 2021: 25, 27, die von PIMS gleichermaßen eine »Verwertungsgesellschaft Daten« umfasst sehen und darauf verweisen, dass Datentreuhänder von PIMS aufgrund vielfältig möglicher Mischformen nicht leicht zu trennen sind. Siehe auch vorige Fußnote und Verbraucherzentrale Bundesverband e.V. 2021: 5 mit der Forderung von technischen Ansätzen, mit deren Hilfe Endnutzer die Speicherung von Informationen in ihren Endeinrichtungen oder den Zugriff auf solche Informationen zentral steuern können. Dies soll auch ein Whitelisting umfassen, das »möglichst einfach« durch die entsprechende Software erfolgen soll, wenn dem Anbieter eines Dienstes eine Einwilligung zur Speicherung von Informationen auf dem Endgerät erteilt wurde. Siehe zur Einführung einer Regelung zu Browsereinstellungen: Die Landesbeauftragte für den Datenschutz Niedersachsen 2021: 2.

32 Auf europäischer Ebene gilt hierfür die von Finnland ausgehende Initiative MyData als Vorreiter, siehe Ministery of Transport and Communications 2015. Kernforderungen sind die Kontrolle der Nutzer über ihre Daten, die Standardisierung der Schnittstellen der jeweiligen teilnehmenden Unternehmen und die Offenheit der Daten (Stiftung Datenschutz 2017: 15 f.).

Diese Instrumente sind ebenso in der Intention des Data Governance Act (siehe oben) abgebildet, der wiederum durch den aktuellen Vorschlag zum EU-Data Act ergänzt wird (Europäisches Parlament 2022). Der Data Act hat das Ziel, den Zugang zu und die Nutzung von Daten durch Unternehmen und Verbraucher zu erleichtern und gleichzeitig Anreize für Investitionen in Möglichkeiten der Wertschöpfung durch Daten zu erhalten. Ziel ist ebenso die Entwicklung von Interoperabilitätsstandards, also von Voreinstellungen, welche eine technische Verbindbarkeit sichern. Gemäß Erwägungsgrund 7 sollte jedoch keine Bestimmung dieser Verordnung so angewandt oder ausgelegt werden, dass das Recht auf den Schutz personenbezogener Daten geschmälert oder eingeschränkt wird.

Gemäß Data Act hat derjenige ein Recht auf Datenzugang und ein Recht auf Datenteilung, der ein Produkt besitzt, least oder mietet (Art. 4, 5 Data Act). Produkte im Sinne des Data Act können etwa Fahrzeuge, Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsgeräte oder landwirtschaftliche und industrielle Maschinen sein, die Daten über ihren Gebrauch oder Umgebung erfassen, erzeugen oder sammeln. Allerdings müssen Anspruchsberechtigte nicht notwendigerweise Betroffene im datenschutzrechtlichen Sinne sein, womit das Recht auf Datenübertragbarkeit gemäß Artikel 20 DSGVO erweitert wird. Das Recht auf »Datenteilung« wird an den Besitz oder zumindest die »wirtschaftliche Investition« angelehnt. Dies entspricht insgesamt nicht mehr der ursprünglichen Idee des Rechts auf Datenübertragbarkeit in der DSGVO, die Monopolstellung von sozialen Netzwerken durch Netzwerkeffekte aufzuweichen und den Wechsel zu datenschutzfreundlichen Technologien zu ermöglichen. Zudem kann ein (kontinuierlicher) Zugriff auf die generierten Daten des Produkts in Echtzeit erfolgen, wenn der Nutzer des Produkts dies verlangt (Art. 5 Data Act).

Im Rahmen des Betroffenenrechts auf Datenübertragbarkeit gemäß Artikel 20 DSGVO hat die deutsche Datenethikkommission allerdings empfohlen, von einer vorschnellen Erweiterung des Portabilitätsrechts auf Portierung in Echtzeit zunächst abzusehen (Datenethikkommission 2019: 21, 137). Dies berücksichtigt der EU-Data Act nicht. Insofern kann an genau diesem Punkt künftig das Recht auf Datenschutz in Widerspruch zu einer damit verbundenen möglichen »Datensouveränität« geraten. Notwendig ist ein solcher Widerspruch aber nicht.

Der Data Act verzichtet des Weiteren auf die Möglichkeit der Teilhabe an den generierten Daten, indem die Nutzer der Produkte (diejenigen, die die Daten generieren) grundsätzlich keine Kompensation erhalten. Dies ent-

spricht zwar der datenschutzrechtlichen Forderung, dass es nicht zu einem »Ausverkauf« von Daten kommen darf. Aber da der Data Act für den Datenhalter eine Kompensation vorsieht (Art. 9 Data Act), bliebe Raum für zusätzliche Gestaltungsmöglichkeiten, um Nutzern eine Teilhabe zu ermöglichen. Dies ließe sich ebenfalls »Datensouveränität« nennen.

## Fazit

Der Bezug auf »das Potenzial von Daten und digitalen Technologien zum Vorteil der Gesellschaft, der Umwelt und der Wirtschaft« einerseits und den Datenschutz sowie Privatsphäre andererseits (Europäischer Rat 2021a: 4), führt auch stets zur Abgrenzung und Abwägung zwischen individuellen und allgemeinen Interessen. Dies wiederum hat zur Folge, dass mit der Diskussion über Datensouveränität stets auch eine Diskussion über Freiheitsrechte, über Mitwirkung sowie Teilhabe und insgesamt über Bürgerrechte verbunden ist.

»Datensouveränität« ist aber gerade nicht nur »informationelle Selbstbestimmung, die eine besondere Perspektive auf die soziale und damit gesellschaftliche Verantwortung von personenbezogenen Daten legt« (Appenzeller/Bretthauer/Birnstill 2021: 173 f.). Eine solche verkürzte Beschreibung von Datensouveränität i.S.d. informationellen Selbstbestimmung greift zu kurz. Sie wird auch dem Konzept des Deutschen Ethikrats nicht gerecht (Deutscher Ethikrat 2018). Datensouveränität betrifft vielmehr die Ebene der Gestaltung. Auf dieser Ebene kann sie dann aber die Vereinbarkeit von Datenschutz mit Interessen der Allgemeinheit sicherstellen. Schutz und Souveränität müssen hier nicht im Widerspruch zueinander stehen.

# Datensouveränität als Privatautonomie

*Florian Möslein und Clara Beise*

## Einleitung

Datensouveränität ist ein schillernder, facettenreicher Begriff, der disziplinenübergreifend Verwendung findet.[1] Insoweit ähnelt er anderen Schlagworten, die sich mit fortschreitender Digitalisierung zunehmend verbreiten, etwa Datenzugang, Dateneigentum, Datenhoheit oder auch digitale Souveränität. Aus rechtswissenschaftlicher Sicht lassen sich beide Wortbestandteile für eine begriffliche Annäherung nutzbar machen. Einerseits geht es um Daten, das heißt um die maschinenlesbar codierte Darstellung von Informationen (Zech 2012: 24–33). Wenngleich Daten Informationen demnach lediglich in Form eines technischen Codes repräsentieren, werden sie im rechtlichen Diskurs häufig mit dem Inhalt dieser Information gleichgesetzt, insbesondere im Datenschutzrecht (»personenbezogene Daten«) (Steinrötter 2017: 732). Datensouveränität reicht begrifflich aber jedenfalls weniger weit als digitale Souveränität (Tiedeke 2021: 624), weil Digitalisierung zwar stark von Daten getrieben wird, aber auch zahlreiche weitere technische Phänomene ohne unmittelbaren Datenbezug umfasst, etwa die Plattformökonomie oder selbst den Fernabsatz. Andererseits geht es um Souveränität, also um Hoheit über Daten. Nun wird der Begriff der Souveränität zumindest in der politischen Theorie zwar häufig staatszentriert verstanden, also im Sinne staatlicher Herrschaft (monographisch Haltern 2007). Solcher Staats- oder Staatengemeinschaftsbezug klingt teils auch an, insbesondere wenn von digitaler Souveränität oder eben auch von Datensouveränität gesprochen wird. Beispielsweise

1 Siehe den Beitrag von Gehring in diesem Band, des Weiteren Martini/Kolain/Neumann/Rehorst/Wagner 2021: 3.

ist im Zusammenhang mit dem Aufbau der föderierten, cloud-basierten Dateninfrastruktur Gaia-X, die den Austausch sowie die wirtschaftliche Nutzung von Daten in einem sicheren Umfeld ermöglichen soll, häufig von europäischer Datensouveränität die Rede (BDI 2021).[2] Indessen bezieht sich der Begriff der Souveränität keineswegs ausschließlich auf staatliche Institutionen, sondern bezeichnet ganz allgemein die Fähigkeit zur Selbstbestimmung, die durch Eigenständigkeit und Unabhängigkeit von Rechtssubjekten charakterisiert wird. Im Zusammenhang mit Daten liegt ein stärker individualisierender Blick besonders nahe, weil es häufig um Daten bzw. Informationen einzelner Rechtspersonen geht, insbesondere eben um personenbezogene Daten.

Bezeichnet Datensouveränität demnach die Selbstbestimmung über Informationen (vor allem) zur eigenen Person, so lässt sich der Begriff als Ausprägung der Privatautonomie verstehen, gleichsam als deren »Übersetzung« ins digitale Zeitalter. Selbstbestimmung als Ausdruck der freien Entfaltung der Persönlichkeit und des individuellen Willens des Menschen (Bydlinski 1996: 147–167; Flume $^{4}$1992: 1–22; Larenz 1979: 57–67; Singer 1995: 39–44; Wolf 1970, 8–31) verkörpert nämlich ein fundamentales Rechtsprinzip, das in den Grundrechten verfassungsrechtlich verankert und in der gesamten Rechtsordnung zu verwirklichen ist, namentlich im Privatrecht als Privatautonomie (Bydlinski 1967: 126–131). Selbstbestimmung fußt auf der Möglichkeit individueller, autonomer Willensbildung und setzt deshalb ein geistes- und naturwissenschaftliches Menschenbild voraus, das von der grundsätzlichen Möglichkeit freier Willensentscheidungen ausgeht (so bereits Fröhlich 1922: 7–30; Gounot 1912). Selbstbestimmung ist umgekehrt ausgeschlossen, soweit die Fähigkeit zu autonomer Willensbildung (»Geschäftsfähigkeit«) ausnahmsweise fehlt oder privates Handeln nicht wirklich freiwillig erfolgt, also nicht auf freiem Willen beruht, sondern beispielsweise auf unmittelbarem Zwang, Drohung oder arglistiger Täuschung (monographisch Gutmann 2001). Im Regelfall verhilft das Prinzip der Selbstbestimmung dem individuellen Willen jedoch umfassend zur Geltung. Privatautonomie darf zur Verfolgung eigener Zwecke und nach eigener Einsicht ausgeübt werden, erlaubt also geradezu »Selbstherrlichkeit« (Reinhardt 1957: 116). Im Zeitalter der Digitalisierung muss dieses privatrechtliche Kernkonzept jedoch neu ausbuchstabiert werden, um Selbstbestimmung im digitalen Raum verbürgen zu können. Der Begriff

2 Siehe auch den Beitrag von Person und Schütrumpf in diesem Band.

der Datensouveränität erscheint geeignet, um als Chiffre dieser Aufgabenstellung zu dienen.

# 1. Datensouveränität als Ausprägung der Privatautonomie

## 1.1 Leistungsfähigkeit des Konzepts der Privatautonomie

Das Konzept der Privatautonomie gibt der Selbstbestimmung des Einzelnen im Rechtsleben Form und Namen (vgl. Flume [4]1992: 1). Es ist verfassungsrechtlich verbürgt und elementarer Bestandteil und Voraussetzung der (Privat-)Rechtsordnung. Die Grundrechte verkörpern dieses Recht auf möglichst weitgehende Freiheit und gebieten gleichzeitig, dass diese Freiheit im Diskurs und in Abstimmung mit der Freiheit anderer auszuüben ist, gleichsam als Gebot »diskursiver Multilateralität« (Wielsch 2013: 752). Nicht das Bestehen von Privatautonomie, sondern ihre Reichweite und ihr relatives Gewicht ist also Gegenstand rechtlicher Abwägungsprozesse.[3] In diesem Sinne ist der Gesetzgeber verpflichtet, der Freiheit des Einzelnen einen »angemessenen Betätigungsraum« (BVerfG, Beschl. v. 19.10.1993 – 1 BvR 567/89) zu schaffen, etwa durch die Bereitstellung von Eigentumsrechten und Gesellschaftsformen, und sie zu begrenzen, wann immer Ungleichgewichtslagen privatautonomes Handeln unmöglich machen.

Der Vertrag ist das zentrale Mittel privatautonomer Gestaltung. Privatautonomie entfaltet sich hier in den Elementen der Abschluss-, Inhalt- und Formfreiheit. Die Freiheit der Einzelperson, ihren natürlichen Willen ursächlich und reflektiert in einer Entscheidung münden zu lassen, darf dabei nicht nur abstrakt bestehen, sondern muss in der konkreten Entscheidungssituation vor Zwang, Täuschung und der Ausnutzung von Unerfahrenheit, mangelndem Urteilsvermögen oder Willensschwäche geschützt werden (»Entscheidungsfreiheit«, vgl. Neuner 2022: 473 ff.).

3 »In den einzelnen Rechtsordnungen wird das Prinzip der Privatautonomie in verschiedenem Umfang verwirklicht. […] Es gibt keine Rechtsordnung ohne Privatautonomie.« (Flume 1992: 1)

## 1.2 Privatautonomie im Digitalen

Die Privatautonomie steht in der Digital- und Datenwirtschaft in besonderer Weise auf dem Prüfstand. Vor allem wenn es um den rechtsgeschäftlichen Umgang mit personenbezogenen Daten geht, offenbaren sich erhebliche wirtschaftliche und informationelle Asymmetrien zwischen der betroffenen Einzelperson und großen Digitalunternehmen. Dieses Ungleichgewicht ist vor allem darauf zurückzuführen, dass Einzelpersonen den Wert »ihrer« Daten nicht einschätzen können, ihn ferner nicht realisieren können, weil sich das Vorhersagepotential durch Skalierung großer Datenmengen ergibt und weil sie schließlich etwaige Rechtspositionen nicht in geeigneter Weise gegenüber den betreffenden Akteuren der Datenwirtschaft durchsetzen können.[4] Anders geht es dagegen den großen Digitalunternehmen. Sie sind wirtschaftlich in der Lage, die Datenanalysen vorzunehmen und verfügen durch ihre Marktposition zwischen Datenerzeugern und Datennutzern über Informationen zu beiden Seiten des Datenmarktes. Um die für beide Marktseiten attraktiven Netzwerkeffekte realisieren zu können, ist ihr Geschäftsmodell gerade auf eine möglichst große Reichweite und Abhängigkeit beider Gruppen gerichtet und trägt somit aktiv zur Aufrechterhaltung monopolartiger Strukturen bei.[5] Damit Einzelpersonen an der Datenwirtschaft in echter Selbstbestimmung teilnehmen und Rechtsbeziehungen gestalten können, müssen Vertragsabschluss-, Gestaltungs- und Formfreiheit auch im Digitalen gewährleistet sein.

Datensouveränität verdeutlicht die Herausforderungen, denen sich Privatautonomie in der Datenwirtschaft stellt, wenngleich der Begriff inhaltlich nicht über das hinaus geht, was Privatautonomie im Digitalen bereits abbildet.[6] Als Buzzword der Digitalisierung findet Datensouveränität gleich-

4 Aus diesem Grund geraten auch Forderungen nach Eigentumsrechten an Daten (Kilian 2002: 921 ff.; Hoeren 2013: 486 ff.; Hoeren 2019: 5 ff.; Zech 2015a: 1151 ff.; Zech 2020: 91 ff.; Fezer 2017: 356 ff.) abgesehen von dogmatischen und wirtschaftlichen Bedenken an ihre Grenzen.

5 »The choice between markets and firms then is not, or is not primarily, a response to transaction costs – but rather a response to the differential ability to create asymmetries of power. « (Pistor 2020: 103)

6 Beachtet man den Bezug und insofern die Begrenzung auf Daten, bleibt der Begriff sogar hinter der Privatautonomie zurück, wann immer digitale Phänomene ohne unmittelbaren Datenbezug in Rede stehen.

wohl breite Verwendung, in der Rechtswissenschaft und darüber hinaus.[7] Wann immer im privatrechtlichen Kontext und in Bezug auf die informationelle Selbstbestimmung von Datensouveränität die Rede ist, muss eine Anbindung an das Konzept der Privatautonomie stattfinden. Datensouveränität ist schließlich eine Übersetzung – und keine Neuerfindung – des in der Privatautonomie zum Ausdruck kommenden Rechtsprinzips in das digitale Zeitalter.

## 2. Dimensionen der Datensouveränität

### 2.1 Abschlussfreiheit

Vertragsabschlussfreiheit hat sowohl eine positive als auch eine negative Dimension. In positiver Hinsicht ist darunter die Freiheit zu verstehen, die eigenen Rechtsverhältnisse durch Vertrag zulässig regeln zu können. Aber auch über den Vertrag und Vertragsstrukturen hinausgedacht, bedeutet Privatautonomie im Digitalen, dass der selbstbestimmte Datenumgang und die Kontrolle des Einzelnen auch auf alternativer Infrastruktur ermöglicht wird.

In negativer Hinsicht umfasst die Dimension der Abschlussfreiheit die Entscheidung, sich nicht vertraglich zu binden oder darüber hinaus generell nicht am Datenrechtsverkehr teilzunehmen. Das Konsenserfordernis ist ein zentraler Bestandteil bei der Gewährleistung dieser negativen Dimension der Vertragsabschlussfreiheit.

#### *2.1.1 Datenvertragsrecht und Daten als Gegenleistung*

Die Digitale-Inhalte-Richtlinie[8] (DI-RL) erfasst unter anderem Verträge, in denen der Verbraucher dem Unternehmer für die digitalen Inhalte oder Dienstleistungen personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt, vgl. Art. 3 Abs. 1 DI-RL. Auch wenn Daten und das digitale Produkt auf diese Weise in eine Austauschbeziehung treten, ordnet die Richtlinie an, dass daraus keine Schlussfolgerung für die Eigenschaft von Daten als Ware gezogen werden kann (vgl. EG 24 DI-RL). Stattdessen sei die

---

7 Siehe hierzu vor allem in diesem Band die Beiträge von Gehring und Augsberg.

8 RL (EU) 2019/770 vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, umgesetzt in den §§ 327 ff. BGB.

Bereitstellung personenbezogener Daten anstelle der Zahlung eines Preises eine faktische Gegebenheit des Digitalmarktes. Verbraucherinnen und Verbraucher sollen, darin liegt der Kerngedanke der Richtlinie, in diesen Konstellationen bzw. »im Zusammenhang mit solchen Geschäftsmodellen« nicht schlechter gestellt werden und insbesondere Anspruch auf vertragliche Rechtsbehelfe haben, die die Richtlinie sodann harmonisierend festlegt (vgl. EG 24 DI-RL). Bezüglich der rechtmäßigen Verarbeitung von Daten gelte aber die Datenschutz-Grundverordnung (DSGVO) erschöpfend, sodass die Richtlinie keine neuen oder verändernden Voraussetzungen für die Datenverarbeitung enthält (vgl. EG 24, 38, Art. 3 Abs. 8 DI-RL). Trotzdem erfahren Austauschbeziehungen mit Daten und mithin Daten als Gegenleistung durch die DI-RL rechtliche Anerkennung.

Das Verständnis von Daten als Gegenleistung (»Bezahlen mit Daten«[9]) steht auch nicht im Widerspruch zum grundrechtlich verbürgten Recht auf Datenschutz.[10] Schließlich umfasst das allgemeine Persönlichkeitsrecht, das den Ursprung des Datenschutzrechts und des Grundrechts auf informationelle Selbstbestimmung bildet (vgl. BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83 u. a.: 147), nicht nur ideelle, sondern auch kommerzielle Interessen (vgl. BGH, Urt. v. 1.12.1999 – I ZR 49/97: 27). Das bedeutet, die Entscheidung des Einzelnen gegen die Erhebung, Speicherung, Verwendung und Weitergabe oder für die Preisgabe und Verarbeitung seiner Daten (vgl. BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83 u. a.: 147) kann auch mit der Motivation erfolgen, hieraus einen Vermögenswert zu realisieren. Das Kommerzialisierungsinteresse bezüglich der eigenen personenbezogenen Daten spiegelt sich auch in der DSGVO wider. Sie legt gerade jene Vorgaben fest, die zum freien Verkehr personenbezogener Daten erforderlich sind und bestimmt, dass der freie Verkehr personenbezogener Daten nicht aus Gründen des Datenschutzes eingeschränkt oder verboten werden darf, vgl. Art. 1 Abs. 3 DSGVO.

Verträge mit und über Daten sind daher grundsätzlich erlaubt. Sobald personenbezogene Daten Vertragsgegenstand werden, findet die DSGVO Anwendung.

---

9 Siehe hierzu jüngst: Schmitz/Buschuew 2022: 171 ff.

10 Auch nicht im Widerspruch zum europäischen Datenschutzgrundrecht Art. 8 GRCh, vgl. Klement 2019: 19; anders dagegen die Andeutung in EG 24 DI-RL.

### 2.1.2 *Datenschutzrechtliche Einwilligung als Konsensmechanismus*

Die Einwilligung ist der zentrale Schutzmechanismus vor ungewollten vertraglichen Beziehungen. Mit der datenschutzrechtlichen Einwilligung findet sich auch im Datenschutzrecht dieses genuin privatautonome Element (vgl. Bunnenberg 2020a: 1088; Bunnenberg 2020b: 29). Die Einwilligungsvoraussetzungen und dabei insbesondere das Recht zum jederzeitigen Widerspruch und das damit verbundene Löschungsrecht (»Recht auf Vergessenwerden«) stärken die Einzelperson in einem Umfang, der eine Strukturähnlichkeit zum dinglichen Herausgabeanspruch aufweist (vgl. Lahusen 2021: 18). Die Besonderheiten der Datenwirtschaft stellen die informierte und freiwillige Einwilligung dennoch vor erhebliche Herausforderungen.

Vertragsbeziehungen liegt die Vorstellung einer grundsätzlichen Verhandlungsparität zwischen den Parteien zugrunde. Diese Vorstellung gerät an ihre Grenzen, wenn die Einzelperson den an ihren Daten interessierten, weil zwei Marktseiten bedienenden, Unternehmen gegenübersteht. Ihr Geschäftsmodell setzt, wie sich gezeigt hat, gerade wirtschaftliche und informationelle Defizite und mithin Abhängigkeiten bei den datengebenden Einzelpersonen voraus. Diese asymmetrische Ausgangslage bleibt nicht ohne Auswirkungen für die Einwilligung und die Frage, ob diese freiwillig und damit wirksam erfolgte, vgl. EG 43 DSGVO. Wird die Einwilligung in die Datenverarbeitung kraft überlegener Marktposition erwirkt, etwa indem der Zugang zu einer Online-Plattform oder einem Online-Produkt an die Einwilligung zur Datenverarbeitung geknüpft wird und das Ausweichen auf andere Vertragspartner mangels Alternative nicht möglich ist, kann an der Freiwilligkeit der erteilten Einwilligung berechtigterweise gezweifelt werden. In dieser Situation hält das Datenschutzrecht das Kopplungsverbot in Art. 7 Abs. 4 DSGVO bereit. Bei der Vorschrift handelt es sich aber um kein absolutes Verbot. Es wird lediglich abgewogen, ob die Einwilligung zur Datenverarbeitung für die Vertragserfüllung erforderlich ist, was Raum für die Berücksichtigung unternehmerischer Interessen lässt (vgl. Bunnenberg 2020b: 261). Eine informierte und freiwillige Einwilligungsentscheidung wird weiter durch die zunehmend komplexen Verarbeitungssituationen und unübersichtlichen Entscheidungsgestaltungen gefährdet (vgl. Martini/Weinzierl 2019: 287 ff.; Bunnenberg 2020b: 111 ff.). Vor diesem Hintergrund entsteht außerdem das als *privacy paradox* bezeichnete Phänomen, bei welchem die individuelle Einstellung zum Datenschutz dem späteren Offenlegungs- bzw. Einwilligungsverhalten widerspricht. Mangels verfüg-

barer oder verständlicher Informationen zu den Kosten und Nutzen der Einwilligung trifft das begrenzt rational agierende Individuum seine Einwilligungsentscheidung unter dem Einfluss kognitiver Verzerrungen (vgl. Martini/Weinzierl 2019: 290 ff.; Bunnenberg 2020b: 100 ff.).

Neben der Einwilligung gibt es weitere Tatbestände für eine rechtmäßige Datenverarbeitung. In der Praxis relevant werden hier vor allem der Tatbestand der Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung, Art. 6 Abs. 1 lit. b DSGVO, sowie der der Datenverarbeitung zur Wahrung berechtigter Interessen, Art. 6 Abs. 1 lit. f DSGVO. Ohne verengende Auslegung (vgl. Bunnenberg 2020a: 1093; Art. 29 WP 2014: 16 f.) kann das Einwilligungserfordernis durch diese in der DSGVO liegenden Gründe weiter geschwächt werden.

Am besten wird eine informierte und freiwillige Einwilligung über Informationspflichten und Transparenz gewährleistet. Die DSGVO sieht hier bereits Rechtsbehelfe, wie Informations- und Auskunftsrechte (Art. 13 ff. DSGVO), die Pflicht zur datenschutzfreundlichen Voreinstellung (Art. 25 Abs. 2 DSGVO) oder das Kopplungsverbot (Art. 7 Abs. 4) vor. Wie sich zeigt, geraten diese Rechtsbehelfe an ihre Grenzen. Sie sind daher durch wettbewerbsrechtliche Regeln zu ergänzen, die Transparenz und faire Verhaltensweisen auf unternehmerischer Seite durchsetzen und die Datenwirtschaft zugunsten der schlechter informierten Einzelpersonen ausbalancieren. Dies geschieht bereits vereinzelt durch Rechtsakte wie die P2B-Verordnung, den Digital Services Act sowie den Digital Markets Act. Das Zusammenspiel aus individuellen Informationsansprüchen und einer transparenten Marktsituation verhilft der Einwilligung wieder zu seiner Funktion als Garant privatautonomen Handelns.

#### *2.1.3 Datenintermediäre*

Einzelpersonen können sich auch entscheiden, über andere Infrastrukturen als durch die unmittelbare vertragliche Beziehung mit Datenverarbeitern an der Datenwirtschaft teilzunehmen, zum Beispiel durch Inanspruchnahme der Dienste eines Datenintermediärs, der sich zur Wahrung ihrer Interessen und zur Stärkung ihrer Rechtsposition verpflichtet hat.[11] Datenintermediäre

11 Darüber hinaus stehen Datenintermediäre auch juristischen Personen zur Verfügung. Nachfolgend werden allerdings die Modelle beleuchtet, die sich auf die Einzelperson und die besondere Lage ihrer Privatautonomie in der Datenwirtschaft konzentrieren.

bringen den Vorteil mit sich, dass sie zwischen Dateninhaber und datenverarbeitende Akteure treten und den Einzelpersonen eine alternative Anlaufstelle bieten, die das strukturelle Ungleichgewicht zwischen ihnen und den großen Digitalunternehmen ausgleicht.

Der Entwurf eines Data Governance Acts (DGA-E) (vgl. Europäische Kommission 2020b) legt die Idee eines Datenintermediärs erstmals gesetzlich fest. Für den Verarbeitungskontext zwischen der Einzelperson und der verarbeitenden Stelle konzipiert der DGA-E den sogenannten Datentreuhänder, Art. 9 lit. b DGA-E, der sich ausschließlich auf personenbezogene Daten konzentriert und dabei beabsichtigt, die Handlungsfähigkeit und Kontrolle des Einzelnen in Bezug auf die ihn betreffenden Daten zu verbessern (vgl. EG 23 DGA-E). Das tut er etwa, indem er die betroffene Person bei der Ausübung ihrer Rechte im Zusammenhang mit den personenbezogenen Daten unterstützt und sie zu Datenverwendungsvorgängen und Datennutzern berät (vgl. EG 23 DGA-E). Die Bindung an die Interessen der betroffenen Personen wird durch treuhänderische Pflichten sichergestellt. Sein Geschäftsmodell gewährleistet, dass keine Anreize zum unfreiwilligen Datenteilen gesetzt werden und dass eine strukturelle Trennung zwischen dem Datenvermittlungsgeschäft und den in diesem Zusammenhang erhaltenen Daten und anderen Geschäftsbereichen besteht (vgl. EG 23, EG 26 DGA-E).

Aus den Vorgaben des DGA-E geht nicht hervor, wie die Beziehung zwischen Einzelperson und Datentreuhänder sowie zwischen Einzelperson und verarbeitendem Unternehmen ausgestaltet und umgesetzt werden soll. Der europäische Gesetzgeber legt ausschließlich einen aufsichtsrechtlichen Rahmen für die Erbringung der Intermediärsdienste fest, um Vertrauen der Dateninhaber für die Inanspruchnahme der Dienste zu wecken (vgl. EG 25 DGA-E). Regelmäßig werden bei den Geschäftsmodellen für Datentreuhänder Prozesse vorliegen, die als Datenverarbeitungsvorgänge die Einwilligung der betroffenen Person erforderlich machen (vgl. Specht-Riemenschneider u. a. 2021: 30 f.). Wenn Datentreuhänder die betroffene Person in ihrer datenschutzrechtlichen Rechtsposition unterstützen sollen, stellen sich Fragen zur Stellvertretung bei der Einwilligung sowie bei der Ausübung der Betroffenenrechte gem. Art. 15 ff. DSGVO. Je nach Konzeption tritt der Datentreuhänder an die Position des Dateninhabers. Bis auf die in Art. 80 Abs. 1 DSGVO genannten Rechte (Art. 77, 78, 79, 82 DSGVO) und für die dort genannten Stellen sieht die DSGVO de lege lata keine zulässige Stellvertretung vor, selbst wenn eine durchsetzungsstarke Stelle

wie der Datentreuhänder viel besser geeignet sein kann, dem Einzelnen die Kontrolle und Selbstbestimmung im Umgang mit den ihn betreffenden personenbezogenen Daten zu ermöglichen (vgl. Specht-Riemenschneider u. a. 2021: 43).

Alternative Strukturen zum Schutz betroffener Personen sind mit dem Grundgedanken der DSGVO vereinbar und zu befürworten. Mit dem Datenportabilitätsrecht hält die DSGVO sogar eine operationelle Grundlage für die Datenvermittlung bereit (vgl. Sattler 2020: 81 f.; DEK 2019: 136). Gesetzgeberischer Handlungsbedarf besteht aber dahingehend, die Idee des Datentreuhänders zu einer realistischen Handlungsoption für die Einzelperson auszubauen. Das bedeutet einerseits einen angemessenen Aufsichtsrahmen zu schaffen und anderseits, das Zusammenspiel zwischen Einzelperson und Datentreuhänder auch in datenschutzrechtlicher Hinsicht zulässig zu gestalten. Nur auf diese Weise wird der Freiheit des Einzelnen Rechnung getragen, an der Datenwirtschaft auch im Zusammenwirken mit einem Datenintermediär teilzunehmen.

## 2.2 Inhaltsfreiheit

Die Freiheit der inhaltlichen Ausgestaltung vertraglicher Beziehungen äußert sich zunächst in der Freiheit, ein Regelungsmodell für den eigenen Sachverhalt auszuwählen (Wahlfreiheit). Die Gestaltungsfreiheit liegt hier kanalisiert vor, als kategorische Freiheit (vgl. Möslein 2011: 53). Die vertragstypologische Erfassung von Rechtsbeziehungen stellt Vertragspartnern eine rechtliche Ausdrucksform zur Verfügung und erzeugt Rechtssicherheit. Dadurch sinken auch die Transaktionskosten (vgl. Zech 2017: 61). Sofern und soweit die Regelungen des gewählten Modells dispositiv sind, können die Vorschriften angepasst, ergänzt oder abbedungen werden, um den Willen der Vertragsparteien bestmöglich abzubilden (Dispositionsfreiheit). Der Raum für Dispositionsfreiheit wird immer dann durch das Recht begrenzt, wenn das Risiko größerer Ungleichgewichte die Chance auf Einzelfallgerechtigkeit bedroht (vgl. Möslein 2011: 56).

### *2.2.1 Vertragstypologische Erfassung von Datenverträgen*

Die DI-RL versperrte sich der vertragstypologischen Einordnung von Verbraucherverträgen über digitale Inhalte und auch sonst sind Verträge über

und im Zusammenhang mit Daten rechtlich nicht erfasst. Ob solche Verträge einen Kauf-, Dienstleistungs- oder Mietvertrag oder einen Vertrag sui generis darstellen, bleibt somit dem nationalen Recht überlassen. Auf diese Weise erhält die Wahlfreiheit eine kollisionsrechtliche Dimension und es entsteht die Grundlage für abweichende und somit grundsätzlich auch konkurrierende Rechtsordnungen im Bereich der Verträge über digitale Inhalte. Die Umsetzung der Richtlinie in das deutsche Recht nimmt ebenfalls keine vertragstypologische Einordnung vor (vgl. BT-Drs. 19/27653: 37 f.). Sowohl die kaufrechtlichen Vorschriften, vgl. § 453 Abs. 1 S. 1, 2 BGB, als auch die Vorschriften zum Dienstvertrag, vgl. § 611 Abs. 2 BGB, können grundsätzlich auf Verträge über digitale Produkte angewendet werden, soweit die §§ 327 ff. BGB keine abschließende Regelung enthalten. Somit wird lediglich ein Teilaspekt des Datenvertragsrechts und zwar jener, der aus verbraucherrechtlicher Sicht relevant ist, gesetzgeberisch ausgestaltet. Im Übrigen besteht Gestaltungsfreiheit, die durch Anleihen aus dem Kauf-, Miet- oder Dienstleistungsrecht wahrgenommen werden kann.

### *2.2.2 Mindeststandards und Inhaltskontrolle*

Die gesetzgeberische Intention bei der DI-RL und ihrer Umsetzung ist vielmehr in der Festsetzung vertraglicher Mindeststandards begründet, um eine Grundlage für privatautonomes Handeln zu schaffen und um den Verbraucher bei Unsicherheit über den erwartbaren Zustand digitaler Produkte sowie der in diesem Zusammenhang bestehenden Rechte zu unterstützen (vgl. EG 5, 8 DI-RL; BT-Drs. 19/27653: 40). Die Unsicherheit und potentielle Unterlegenheit des Verbrauchers ist nicht darauf zurückzuführen, dass er als Verbraucher per se unterlegen und als schwächere Vertragspartei schutzwürdig ist. Vielmehr verhindert die zwischen dem Verbraucher und seinem Vertragspartner bestehende Informationsasymmetrie und das in diesem Zusammenhang drohende partielle Marktversagen privatautonomes Handeln (vgl. Basedow 2019: 6; Leyens/Schäfer 2010: 782 ff.). Gerade in der Datenwirtschaft verstärkt sich die informationelle Ungleichgewichtslage, weil die Bepreisung von Daten sich an keinen Marktsignalen orientieren kann. Die Informationskosten stehen regelmäßig außer Verhältnis zu ihrem Nutzen, sodass es aus rationalen Gesichtspunkten geboten ist, keine Informationsanstrengungen zu unternehmen. Diese Ausgangslage setzt keine Anreize für fair bzw. datenschutzfreundlich agierende Vertragspartner. Sie verlassen den Markt und eine Verschlechterung des Marktstandards

droht (vgl. Akerlof 1970: 488 ff.). Mindeststandards begrenzen die Informationsasymmetrie, die Vertragsgestaltungen vor diesem Hintergrund prägt.

Ähnliches bezweckt die gesetzliche Inhaltskontrolle, wenngleich auf einer konkreten, individualvertraglichen Ebene. Bis auf § 138 BGB ist das Verhältnis von Leistung und Gegenleistung allein dem Verhandeln der Marktakteure überlassen und der gesetzlichen Nachprüfung entzogen. Bei Daten als Leistungsgegenstand versagt allerdings der Markt als Richtigkeitsgewähr, sodass die Datenüberlassung in bestimmtem Umfang kontrollfähig ist (vgl. Hacker 2019: 184 ff., 188). Die DSGVO hält daher mit Art. 7 Abs. 4 DSGVO und dem Erfordernis der informierten Einwilligung, Art. 4 Abs. 1 Nr. 11 DSGVO, Kontrollmechanismen bereit. Das Transparenzgebot stellt sicher, dass die betroffene Person den Datenverarbeitungsvorgang nachvollziehen kann und Verarbeitungszweck und verarbeitende Stelle kennt. Art. 7 Abs. 4 DSGVO enthält als Tatbestandsvoraussetzung einer wirksamen Einwilligung gleich zwei Kontrolldimensionen. Die Vorschrift fungiert als Überraschungskontrolle, indem sie der betroffenen Person Datenverarbeitungsvorgänge vor Augen führt, mit denen sie nicht rechnen musste (vgl. Bunnenberg 2020a: 1096). Ergänzend wird die beabsichtigte Datenverarbeitung einer Angemessenheitskontrolle unterzogen. Unzulässig sind danach Datenverarbeitungen, die zu einer unzumutbaren Belastung der betroffenen Person führen, etwa indem sie in keinem vertretbaren Verhältnis zur Gegenleistung stehen (vgl. Bunnenberg 2020a: 1096; Hacker 2019: 186 ff.). Für die Abwägung relevant werden die Dauer, Intensität und Reichweite der Datenverarbeitung, die Art der betroffenen Daten und ihre semantische Nähe zu diskriminierungsgefährdeten Grundrechten.

Gesetzliche Mindeststandards und die vertragliche Inhaltskontrolle schränken die Gestaltungsfreiheit zwar ein, sie sichern zugleich aber auch selbstbestimmtes Handeln. Mindeststandards schaffen Vertrauen in bestimmte Vertragsgestaltungen, indem sie ein Zurückfallen auf ein Schutzniveau garantieren und Orientierung bei der Einschätzung der Rechten- und Pflichtenlage bieten. Die Inhaltskontrolle stellt bei einem konkreten Datenverarbeitungsvorgang sicher, was der Markt und gesetzliche Mindeststandards gerade in der diffizilen Situation der Datenwirtschaft nicht abbilden kann, und zwar, dass sich die Vertragsgestaltung in einem angemessenen und transparenten Rahmen bewegt.

### *2.2.3 Dispositives Datenvertragsrecht*

Auf der anderen Seite drückt sich privatautonome Gestaltung von Rechtsbeziehungen in Forderungen nach Handlungsspielräumen in gesetzlichen Bestimmungen aus. Vor allem die DSGVO, die den Verkehr personenbezogener Daten anerkennt und ermöglicht, schränkt die freie Gestaltung dieser Beziehungen dennoch erheblich ein. Ihr sachlicher Anwendungsbereich ist eröffnet, wenn es um die Verarbeitung personenbezogener Daten geht. Eine Vielzahl von Daten können einen Personenbezug begründen,[12] sodass schon die Rechtsunsicherheit in Bezug auf den Anwendungsbereich die Gestaltungsfreiheit erheblich einschränkt (vgl. Sattler 2020: 65).

Zentraler Erlaubnistatbestand für die Datenverarbeitung ist die Einwilligung, deren Rechtmäßigkeit an Voraussetzungen gebunden ist. Der Zweckbindungsgrundsatz gibt vor, dass der Zweck der Datenverarbeitung zum Zeitpunkt der Einwilligung bestimmt sein muss, weshalb generell erklärte Einwilligungen oder Weiterverarbeitungsvorgänge de lege lata ausgeschlossen sind. Art. 6 Abs. 4 DSGVO sieht mit der Vereinbarkeitsprüfung zwar eine gesetzliche Ausnahme vom Zweckbindungsgrundsatz vor, allerdings in Form einer Einzelfallabwägung, die wenig Rechtssicherheit schafft. Schließlich sorgt die Reichweite des Kopplungsverbots bzw. des Berücksichtigungsgebots in Art. 7 Abs. 4 DSGVO für Unsicherheiten bezüglich der verbleibenden Gestaltungsfreiheit (vgl. Riehm 2020: 182). Es darf durch die Verknüpfung von Leistung und Einwilligung in die Datenverarbeitung weder unmittelbar noch mittelbar der Eindruck eines rechtlichen Zwangs oder einer Verpflichtung entstehen, da andernfalls die Freiwilligkeit der Einwilligung in Frage gestellt ist (vgl. Riehm 2020: 196). Aus gleichen Gründen kann das Recht zum jederzeitigen Widerruf der Einwilligung, Art. 7 Abs. 3 S. 1 DSGVO, vertraglich nicht begrenzt oder abbedungen werden. Es ist untrennbar mit der Einwilligung verbunden. Das Widerrufsrecht beeinträchtigt aber in erheblichem Umfang das Vertrauen der anderen Vertragspartei in die Verbindlichkeit getroffener Vereinbarungen. Auch wenn der Widerruf die Datenverarbeitung nicht rückwirkend, sondern nur für die Zukunft unwirksam macht, beschränkt er vertragliche Gestaltungsmöglichkeiten und setzt überdies Anreize zum schnellen Datenweitertransfer (vgl. Sattler 2020: 80).

---

12 Siehe etwa das weite Verständnis (potentieller Personenbezug) des EuGH, in: Urteil vom 19.10.2016 – C-582/14 (Breyer/Deutschland).

Ebenfalls wenig Dispositionsspielraum lässt die DSGVO bei der Frage der Stellvertretung bei Einwilligung, Widerruf und bei den Betroffenenrechten, obwohl die Stellvertretung durch ausgewählte und spezialisierte Dritte zu einer im Ergebnis besseren Rechtsposition der betroffenen Einzelperson führen kann (vgl. Specht-Riemenschneider u. a. 2021: 44). Kann sich die Einzelperson bei der Geltendmachung ihrer Rechte nicht durch eine Person vertreten lassen, von der sie sich wegen ihrer strukturellen Größe, ihrer Professionalisierung oder technischen Infrastruktur eine effizientere Rechtsdurchsetzung verspricht, liegt hierin eine erhebliche Beschränkung privatautonomen Handelns.

Gesetzgeberisches Tätigwerden ist daher angezeigt, um privatautonome Vertragsgestaltungen zu ermöglichen. Im Zentrum der Überlegungen sollte die Weiterentwicklung der Einwilligung stehen, beispielsweise durch die Anerkennung einer flexiblen Einwilligungslösung, die es der betroffenen Person ermöglicht, unabhängig von einem konkreten Anlass Einwilligungspräferenzen für verschiedene Verarbeitungsvorhaben festzulegen (vgl. Specht-Riemenschneider u. a. 2021: 41). Ferner sollte erwogen werden, über die bestehenden Regeln der DSGVO hinaus Stellvertretung bei der Wahrnehmung und Ausübung der Einwilligung und der Betroffenenrechte zu ermöglichen.[13]

## 2.3 Formfreiheit

Flankierend prägt schließlich die Formfreiheit die Privatautonomie, indem sie die Abschluss- und Inhaltsfreiheit effektiv absichert. Formale Anforderungen erhöhen nämlich die Transaktionskosten und können daher die privatautonome Gestaltung rechtlicher Beziehungen beeinträchtigen. Im deutschen Recht herrscht deshalb grundsätzlich Formfreiheit: Verträge können im Regelfall ohne Einhaltung einer bestimmten Form geschlossen werden; die zentralen rechtsgeschäftlichen Vorschriften der §§ 145 ff. BGB machen für Antrag und Annahme keinerlei Formvorgaben (Möslein 2019a: Rn. 36). Jedoch statuiert das Gesetz für bestimmte Rechtsgeschäfte spezifische Formerfordernisse, teils zum Zwecke der Warnung und des Übereilungsschutzes, teils (zusätzlich) zu Klarstellungs- und Beweiszwe-

13 Datentreuhänder als »verlängerter Arm« der betroffenen Person (vgl. Specht-Riemenschneider u. a. 2021: 41 ff., 45).

cken (Busche 2021: Rn. 30; Musielak 2017: 952). Die wichtigsten Formen, die von entsprechenden Rechtsvorschriften verlangt werden, sind die notarielle Beurkundung bzw. öffentliche Beglaubigung gem. §§ 128 f. BGB, die Schrift- und die mit ihr gleichgestellte elektronische Form gem. §§ 126, 126a BGB sowie die Textform gem. § 126b BGB. Auch wenn solche Formvorgaben die Privatautonomie auf den ersten Blick beschränken, lassen sie sich gleichwohl durchaus als freiheitsschützend rechtfertigen, weil sie den Parteien beispielsweise Gelegenheit zu gründlicher Überlegung geben und zugleich die Rechtssicherheit erhöhen.

Im digitalen Zusammenhang und insbesondere im Datenkontext ist die Formfreiheit in zweierlei Hinsicht relevant. Einerseits stellt sich vielfach die Frage, ob Formerfordernisse die Einsatzmöglichkeiten digitaler Kommunikation bei Abschluss von Verträgen beschränken, ob also beispielsweise E-Mails herkömmlichen Schriftformerfordernissen genügen. Die Privatautonomie als Möglichkeit des Einzelnen, seine Rechtsverhältnisse nach dem eigenen Willen zu gestalten, umfasst grundsätzlich auch die Freiheit, Rechtsgeschäfte mit Mitteln elektronischer Kommunikation abzuschließen. Systematisch hat diese Dimension der Privatautonomie Bezüge zur Abschluss- wie auch zur Formfreiheit, weil sie einerseits die Wahl des Vertragspartners unabhängig von dessen räumlicher Nähe oder eben Distanz ermöglicht, und weil sie andererseits von analogen Formalien wie dem sprichwörtlichen Handschlag befreit (Möslein 2020: 1011). Entsprechend ermöglicht die Privatautonomie den Parteien ferner, sich in Form eines Programmcodes zu binden: Private Akteure können daher auch per blockchainbasiertem Smart Contract kontrahieren (Möslein 2019b: 267 f.; Kaulartz 2016a: 1028 f.; Kaulartz 2016b: 204). Ähnlich wie die Privatautonomie selbst lässt sich auch die Freiheit, Rechtsgeschäfte mit Mitteln elektronischer Kommunikation abzuschließen, auf deren grundrechtliche Verankerung in Art. 1 Abs. 1, 2 Abs. 1 GG zurückführen (Di Fabio 2020: Rn. 101 f.). Entsprechend führt der Gesetzgeber immer wieder neue Formerweiterungen ein, um Rechtsgeschäfte in digitaler Form zu ermöglichen: So bietet § 126a BGB bereits seit 20 Jahren (Riehm 2021: 71 f.) die Möglichkeit, die Schriftform insbesondere beim Vertragsschluss durch elektronisch signierte digitale Dokumente zu ersetzen; neben der Schriftform haben auch die §§ 126b, 127 BGB den elektronischen Vertragsschluss deutlich erleichtert. Im Bereich des Wertpapierrechts können papiergebundene (Sammel-)Urkunden hingegen erst seit kurzem, nämlich seit Inkrafttreten des Gesetzes über elektronische Wertpapiere am 10. Juni 2021, durch Eintragungen in elektronische Regis-

ter ersetzt werden; zudem wurde diese Möglichkeit vorerst nur für eine bestimmte, sachlich eng begrenzte Kategorie von Wertpapieren eröffnet (Möslein 2022: Rn. 11 ff.; Möslein 2021a: 190 ff.). Privatautonomie erfordert somit immer wieder die Fortentwicklung von Formerfordernissen, um Rechtsgeschäfte in digitaler, datenbasierter Form zu ermöglichen.

Andererseits können datenbezogene Rechtsgeschäfte auch neue, zusätzliche Formvorgaben erfordern, weil neue Schutz- und Informationsbedürfnisse entstehen. Bereits beim Fernabsatz gelten beispielsweise zusätzliche Informationspflichten (vgl. § 312d BGB iVm Art. 246a EGBGB und Kramme 2015). Für die datenschutzrechtliche Einwilligung bestehen nach den Regeln der DSGVO zwar keine Formvorschriften; sie kann also mündlich, schriftlich oder elektronisch erfolgen. Gemäß Art. 7 Abs. 1 DSGVO gilt jedoch eine Dokumentationspflicht, nach der Unternehmer auf Nachfrage die Einwilligung der jeweiligen Nutzer nachweisen können müssen (Uecker 2019: 249). Zu beachten sind zudem die Formvorgaben für den Widerruf der Einwilligung durch den Nutzer: Gemäß Art. 7 Abs. 3 S. 4 DSGVO muss der Widerruf der Einwilligung genauso einfach sein wie deren Erteilung (Ernst 2020). Ein weiteres Beispiel für datenbezogene Formerfordernisse liefert Art. 22 DGA-E, der ein europaweit einheitliches Einwilligungsformular vorsieht, um das Sammeln von Daten auf der Grundlage des Datenaltruismus zu erleichtern (Hartl/Ludin 2021: 537). Insgesamt zeigt sich, dass auch in der Datenökonomie Formerfordernisse eine wichtige Rolle spielen, um Privatautonomie – und hier ganz buchstäblich Datensouveränität, nämlich die selbstbestimmte Entscheidung über die Nutzung der eigenen Daten – effektiv abzusichern.

## 3. Zusammenfassung

Datensouveränität bezeichnet die Selbstbestimmung über Daten. Sie lässt sich als Ausprägung der Privatautonomie und als deren »Übersetzung« ins digitale Zeitalter verstehen, weil in der Datenwirtschaft zunehmend (personenbezogene) Daten Gegenstand oder Gegenleistung vertraglicher Beziehungen werden. Da die Privatautonomie infolge von Ungleichgewichten zwischen betroffenen Einzelpersonen und Digitalunternehmen auf dem Prüfstand steht, bringt der Ruf nach Datensouveränität zugleich die spezifischen Herausforderungen zum Ausdruck, denen sich Privatautonomie in der Datenwirtschaft stellen muss.

So verstandene Datensouveränität lässt sich in drei Dimensionen entfalten. Erstens beinhaltet Privatautonomie die Abschlussfreiheit, die in ihrer negativen Dimension auch die Entscheidung umfasst, sich nicht vertraglich zu binden. Entsprechend ist die Einwilligung als wichtigster Schutzmechanismus gegen ungewollte Vertragsbeziehungen und im Fall der Datenwirtschaft als Schutz vor ungewollter Datenverarbeitung zentral für privatautonomes Handeln. Damit die Einwilligung auf freiwilliger und informierter Basis erteilt wird, sind individuelle Informationsrechte um Marktverhaltensregeln und Transparenzpflichten für die Akteure der Datenwirtschaft zu ergänzen. Datensouveränität umfasst zweitens Inhalts- bzw. Gestaltungsfreiheit. Sie muss gewährt werden, um Einzelpersonen zum Beispiel zu ermöglichen, über alternative Strukturen wie Datentreuhänder am Datenverkehr teilzunehmen, ohne dass die Vorgaben der DSGVO oder aufsichtsrechtliche Bestimmungen Datentreuhandmodellen entgegenstehen. Gestaltungsfreiheit muss auf der anderen Seite zurückgenommen werden, wenn die Grundvoraussetzungen für selbstbestimmtes Handeln wegen Informationsungleichgewichten und dem fehlenden Korrektiv des Marktes nicht gegeben sind. Drittens schließlich beinhaltet Privatautonomie Formfreiheit, die im Fall der Datenwirtschaft auch die Freiheit umfasst, Rechtsgeschäfte mit Mitteln elektronischer Kommunikation oder ansonsten in digitalen Formen abzuschließen. Im Zuge der Digitalisierung bedarf es deshalb auch gesetzlicher Formerweiterungen. Umgekehrt erfordern datenbezogene Rechtsgeschäfte teils neue, zusätzliche Formvorgaben, weil andersartige Schutz- und Informationsbedürfnisse entstehen. Formerfordernisse spielen auch in der Datenwirtschaft eine wichtige Rolle, um Datensouveränität effektiv abzusichern.

# Datenschutz, Datensouveränität, Data Governance: Überlappungen, Spannungen und mögliche Lerneffekte

*Steffen Augsberg*

## 1. Daten als zentraler Faktor der Netzwerk-/Plattformgesellschaft

Digitalisierung bedingt Datafizierung. Je stärker wir unsere offline- und online-Existenz verschränken, desto mehr nachvollziehbare und deutbare Spuren hinterlassen wir. Das erhöht das Risiko, über die umfassend vorhandenen, mittels neuer technischer Mittel vielfach miteinander verknüpfbaren Daten weitreichende Informationen über Einzelne zu erlangen und damit letztlich deren Lebensgestaltung beeinflussen zu können. Typische Entwicklungstrends lassen sich mit den Schlagworten Vernetzung und Hyperinformation, Enträumlichung und De- bzw. Transhumanisierung, aber auch zunehmender Präzision und Prognosefähigkeit beschreiben. Die Regulierung des Datenflusses im Sinne von dessen Kontrollierbarkeit (auch) durch die Datengeber dient dem Schutz einer freiheitlichen, selbstbestimmten Lebensführung. Schon deshalb besteht ersichtlich ein erhebliches Interesse daran, effektive Steuerungsformen einzusetzen. Gleichzeitig handelt es sich erkennbar um ein besonders dynamisches Regelungsumfeld. Dies betrifft nicht allein den rasanten technologischen Fortschritt, sondern zumal dessen komplexe Auswirkungen auf das gesellschaftliche Umfeld, das menschliche Miteinander und letztlich unser Selbstverständnis. Es geht nicht um eine Momentaufnahme oder einen auf bestimmte Teilbereiche beschränkten Effekt. Vielmehr erleben wir einen umfassenden Transformationsprozess, dessen Ende und Ergebnis noch nicht absehbar sind. Dieser Einsicht entspricht eine regulatorische und gestalterische Herangehensweise, die den tatsächlichen Entwicklungen Rechnung trägt, basale, unverändert gültige normative Vorgaben identifiziert und hinreichend adaptive Durchsetzungsmechanismen etabliert.

Zugleich ist darauf zu achten, nicht durch allzu rigide und unflexible Mechanismen die Chancen zu verspielen, die mit intensivierter Datennutzung verbunden sind. Es geht, um ein häufiger benutztes Wortspiel aufzugreifen, darum, den Datenschutz und den Datenschatz in ein angemessenes, den modernen Verhältnissen entsprechendes, realistische Hoffnungen wie Risiken austarierendes Verhältnis zu bringen. Ersichtlich sind hierfür eine Vielzahl schwieriger, auch in ihren tatsächlichen Grundlagen noch nicht restlos erschlossener Fragen zu beantworten: Welchen Grad an Kontrolle, Offenheit und Transparenz halten wir für sinnvoll bzw. akzeptabel? Welche Kontrollverluste sind umgekehrt im Interesse zu erwartender Vorteile hinnehmbar, und wer zeichnet für diese Entscheidungen verantwortlich? Zu klären ist ferner, wie mit der durch Selbstvermessungsinstrumente (wie Smartphones und -watches) erzeugten selbstveranlassten Fremdbestimmung umzugehen ist, ob bzw. wie tradierte Autonomieansprüche und Verantwortungszuschreibungen auch gegenüber algorithmenbasierten Entscheidungen Relevanz behalten können und wie es sich auf die normativen Grundannahmen einer zumindest partiell bewusst ignoranten Gesellschaft auswirkt, wenn durch KI-gestützte Datenanalysen eine prädiktive Präzision erreichbar wird, die gängige (Un-)Gewissheitsvorstellungen überholt erscheinen lässt. Genauere Gefahren- und Risikoeinschätzungen, aber auch allgemeine Verlaufs- und Entwicklungsprognosen eröffnen neue Möglichkeiten der Zukunftsgestaltung. Will man diese wahrnehmen, müssen die herkömmlichen Verfahren nicht pauschal ersetzt werden. Sie können aber mit den neuen Erkenntnismethoden sinnvoll ergänzt und sowohl effektiver als auch effizienter gestaltet werden.

Um sicherzustellen, dass die zweifelsohne bestehenden Chancen genutzt werden können, ohne inakzeptable Risiken in Kauf zu nehmen, müssen unterschiedliche Gestaltungs-, Regulierungs- bzw. Governance-Optionen in den Blick genommen werden. Ein bloßes »Weiter so!« ist ersichtlich ebenso wenig sinnvoll wie eine vorhandene Erfahrungen ignorierende grundstürzende Neuordnung. Statt dessen ist nach konkreten Leitbildern zu fragen, die geeignet sind, eine dem Regelungsgegenstand adäquate Strategie zu begründen, die Weiterentwicklungen anleitet und auf Herausforderungen aktiv reagiert. Einen entsprechenden Vorschlag, der sich schlagwortartig auf den Begriff der Datensouveränität reduzieren lässt, hat Ende 2017 der Deutsche Ethikrat unterbreitet (Deutscher Ethikrat 2018). Dieser Vorschlag ist im Folgenden, unter anderem auch in den Beiträgen dieses Bandes, kontextualisiert, kritisch hinterfragt (vgl. etwa Kühling 2020) und weitergeführt

(Hummel u. a. 2021a) worden. Er wird im Folgenden mit zwei weiteren Regelungskonzeptionen in Verbindung gebracht. Meine These ist dabei, dass die drei getrennt voneinander vorzustellenden Ansätze sich in den verfolgten Grundanliegen und den dafür eingesetzten Mitteln unterscheiden, aber es sich dennoch nicht notwendig um alternative, sondern zumindest auch um komplementäre Vorgehensweisen handelt.

## 2. Datenschutz: klassische Schutzmechanismen und ihre Grenzen

Datenschutz beschreibt im hier verstandenen Sinne die klassische, zunächst nationalstaatlich und später auf Ebene der Europäischen Union rechtlich abgesicherte Vorstellung,[1] dass personenbezogene Daten jedenfalls grundsätzlich der Hoheit derjenigen unterliegen, auf die sie sich primär beziehen. Es geht damit nicht unmittelbar um den Schutz der Daten als solcher, sondern mittelbar um den Schutz der Privatsphäre bzw. der informationellen Selbstbestimmung der Datengeber. Diese Grundwerte äußern sich demnach in einer Reihe konkreter Rechte, die Einzelpersonen in Bezug auf »ihre« personenbezogenen Daten zugewiesen werden. Das ist kein Eigentum im rechtstechnischen Sinne. Es weist aber – wie Abwehrrechte insgesamt – starke Parallelen zum Grundmodell eines absoluten Ausschlussrechts auf. Dieser Logik entspricht es, dass anonymisierte/pseudonymisierte Daten als weniger problematisch erachtet werden als solche, die einfache Rückverfolgbarkeit ermöglichen. Sie schlägt sich ferner nieder in allgemeinen Grundsätzen, die insbesondere die Datensparsamkeit/Datenminimierung, die prinzipielle Einwilligungsbasiertheit der Datennutzung und ein relativ strenges Zweckbindungskonzept umfassen. Ausnahmen betreffen insbesondere die Erfüllung von Verträgen und gesetzliche Erlaubnistatbestände; hier stellen sich spezifische Fragen und bestehen Unklarheiten etwa mit Blick auf die einschlägigen »berechtigten Interessen« und die Reichweite von Privilegierungsvorschriften. Im Einzelnen besteht eine Vielfalt an Rechten, die individuelle Kontrolle absichern sollen. Zu ihnen zählen etwa Regelungen zur Datenübertragbarkeit, Löschungs- und Berichtigungsansprüche und mehr. Dass die Verarbeitung personenbezogener Daten grundsätzlich die Zustim-

1 Zur Entwicklung: Kühling 2014; als kurzer Überblick: Leeb/Liebhaber 2018.

mung des Betroffenen voraussetzt (vgl. näher Ernst 2017), bildet den Kernbestandteil einer Opt-in-Herangehensweise, deren modernere Ausprägung die Forderung nach »privacy by design« bzw. »privacy by default« ist – datenminimierende und datenschutzoptimierende Einstellungen sollen nicht erst mühsam herstellbar sein, sondern im Gegenteil: Abweichungen von diesem Standard müssen begründet werden (dazu Mantz [2]2018). Das ist schon deshalb eine spannende (Weiter-)Entwicklung, weil damit technische und rechtliche Anforderungen im Sinne einer Anpassung an technischen Fortschritt verschränkt werden.

Dennoch deutet eine kritische Analyse des Datenschutzrechts auch nach den jüngeren Änderungen, namentlich der Datenschutzgrundverordnung (DSGVO) und den hierauf bezogenen deutschen (Datenschutz-)Gesetzen, darauf hin, dass die vorhandenen Bestimmungen mit Blick auf kurrente Datenverarbeitungsmöglichkeiten (»Big Data«) spezifische Defizite und Dysfunktionalitäten aufweisen. Es handelt sich nicht um ein überholtes, aber doch jedenfalls um ein überarbeitungsbedürftiges Konzept. Typisch für Big Data ist eine konsequente und kontinuierliche De- und Rekontextualisierung unterschiedlichster Daten. Infolge insbesondere der verbesserten Dateninfrastruktur können sehr große und vielfältige Datenmengen in sehr hoher Geschwindigkeit, teilweise in Echtzeit, effektiv erfasst und miteinander kombiniert werden – die dabei erkennbaren Muster erlauben Erkenntnisse, die nur teilweise erwart- und vorhersehbar sind. Damit stehen zumindest einige grundlegende Prinzipien und Instrumente (etwa: enge Einwilligungsmodelle, Erhebung nur minimaler Datenmengen) in deutlichem Widerspruch zu Big-Data-Anforderungen (flexible Datenanbindung, große Datensammlungen außerhalb klar definierter Zwecke). Folglich besteht ein spürbares Spannungsverhältnis zwischen Big Data/KI und dem geltenden Datenschutzrecht. Die Effektivität der bisherigen Schutzmechanismen erscheint damit zweifelhaft. Geht man indes davon aus, dass Big-Data-Anwendungen faktisch vorhanden sind und zudem sinnvoll eingesetzt werden können, dann bedarf es neuer, angepasster Verfahren, die den weiterhin grundlegenden normativen Vorgaben entsprechen und ihnen zur Durchsetzung verhelfen: Freiheit und Selbstbestimmung, Privatheit und Intimität, Souveränität und Macht, Schadensvermeidung und Wohltätigkeit sowie Gerechtigkeit, Solidarität und Verantwortung (vgl. Deutscher Ethikrat 2018: 128 ff.; Hummel u. a. 2021a: 11 ff.).

Spezifische Probleme bestehen zudem bei bereichsspezifischen Datenschutzbestimmungen (etwa: Gesundheitsdatenschutz und Sozialdaten-

schutz, aber auch Finanzdaten). Hier ist, erstens, in faktischer Hinsicht zu fragen, ob diese Abgrenzungen angesichts der gegenwärtigen Entwicklungen von »Big Data« und »Machine Learning« aufrechterhalten werden können. Unter diesen relativ neuen Bedingungen verlieren pauschale Zuordnungen zu einem bestimmten Lebensbereich, aber noch weitergehend auch die Vorstellung besonderer Sensibilitäten an Plausibilität. Das gilt zumal, als sich die Modi der Datenerhebung, also die sogenannten Datenquellen, massiv verändert haben: Die traditionelle, bewusste und zweckgerichtete Datenerhebung durch die späteren Datenverwender verliert an Bedeutung. Zunehmend werden große Datenmengen durch die Individuen selbst generiert, erfasst und weitergeleitet – etwa über die Sensoren und Apps von Mobiltelefonen und am Körper getragenen Geräten (Fitness-Tracker, Smartwatches).

Zweitens ist die Vorstellung eines sektorspezifischen Datenschutzrechts in normativer Hinsicht fragwürdig geworden. Zwar mag es prima facie sinnvoll erscheinen, für bestimmte Domänen Datenschutzvorgaben im Detail angepasst auszugestalten. Die DSGVO enthält diese Differenzierung jedoch gerade nicht. Sie bezieht sich zwar an verschiedenen Stellen auf gesundheitsbezogene Daten und sieht zudem wiederholt Privilegierungen für die Forschung vor. Sie ist allerdings wesensgemäß dadurch gekennzeichnet, dass sie einen übergreifenden, einheitlichen Schutzstandard verlangt. Mit Blick auf die vorhandenen, diesen Aspekt jedenfalls nicht explizit erfassenden Öffnungsklauseln sprechen gute Gründe dafür, dass die DSGVO einer weiterreichenden bereichsbezogenen Unterscheidung prinzipiell widerstreitet.

## 3. »Datensouveränität als informationelle Freiheitsgestaltung«

Das beschriebene, klassische Modell des Datenschutzes sieht sich sowohl durch Neu- und Weiterentwicklungen technischer Natur als auch durch hierauf reagierende normativ-konzeptionelle Reformvorschläge herausgefordert. Zu den in der jüngeren Vergangenheit am intensivsten diskutierten Konzepten gehört die »Datensouveränität«. Sie wird teilweise recht pauschal als Frontalangriff auf das gängige Datenschutzmodell verstanden. In diesem Sinne äußerte sich etwa die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, die forderte,

»das Verbotsprinzip nach der DSGVO nicht durch den Anspruch auf ›Datensouveränität‹ aufzuweichen. Datensouveränität ist ein Schlagwort in der politischen Auseinandersetzung um die zeitgemäße Positionierung des Datenschutzes, das in unterschiedlichen Zusammenhängen gebraucht wird. Aus der Alltagssprache entnommen, wird der aus dem Staatsrecht stammende Begriff Souveränität mit selbstbestimmtem Handeln assoziiert, der einen Anspruch auf (absolute) Herrschaft über die eigenen persönlichen Daten beinhaltet. Dies allerdings kommt nach gegenwärtigem Rechtsverständnis allenfalls im Kernbereich privater Lebensgestaltung in Betracht. Zudem trifft er datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern. Die DSK spricht sich daher dafür aus, auch künftig das aus der Menschenwürde abgeleitete Recht auf informationelle Selbstbestimmung in den Mittelpunkt zu stellen und bei dem funktionalen Begriff des datenschutzrechtlichen Verbotsprinzips zu bleiben.« (Datenschutzkonferenz 2017a)

Demgegenüber ist darauf zu verweisen, dass das Datensouveränitätsmodell keineswegs eine Absage an den Datenschutz darstellen muss, sondern im Gegenteil dessen Grundgedanken in einer neuen, technologisch avancierteren Umwelt aufrechtzuerhalten versucht. Knapp zusammengefasst laufen entsprechende normative Überlegungen auf die Forderung hinaus, ein neues, der Komplexität und Entwicklungsdynamik von Big Data und KI angemessenes Governancemodell zu entwickeln. Datensouveränität gilt dem Deutschen Ethikrat als zentrales Leitprinzip für eine solche Neuorientierung – er definiert sie als eine den Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung (vgl. Deutscher Ethikrat 2018: 51). Diese Begriffsbildung verweist auf das bekannte Konzept der informationellen Selbstbestimmung, setzt sich aber zugleich von ihm ab. Informationelle Freiheitsgestaltung in diesem Sinne meint interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt.

Für das durch den Ethikrat artikulierte Souveränitätsverständnis nimmt die Stellungnahme *Big Data und Gesundheit* explizit stärker individualisierte Souveränitätsbezüge in Bezug, die in philosophischen Untersuchungen mit Blick auf die menschliche Leiblichkeit formuliert werden. Obschon das Souveränitätsparadigma selbstredend gerade im Kontext biopolitischer Analysen große Bedeutung besitzt (vgl. Foucault 2004: 161: »Das Problem der Souveränität ist nicht eliminiert; es ist im Gegenteil akuter denn je geworden.«), findet sie hier einen spezifischen, von traditionellen staatsphilosophischen Verwendungsformen distinkten Anwendungsbereich. Insbesondere in der Auseinandersetzung mit der »souveränen« Verfü-

gung über den (eigenen) Körper – etwa mit Blick auf die Beendigung des eigenen Lebens oder, ganz aktuell, die individuelle und gegebenenfalls Festlegung geschlechtlicher Zugehörigkeit – zeigen sich interessante, spannungsreiche Begriffskonkretisierungen. Das betrifft etwa die Frage nach der Absolutheit des Souveränitätsanspruchs respektive dessen Bindung an bestimmte lebensweltliche Voraussetzungen. Während insoweit einerseits vor bedenklichen Biologismen gewarnt wird und souveräne (oder auch: autonome, selbstbestimmte – die Terminologie variiert) Entscheidungsbefugnisse über als bloße soziale Konstruktionen wahrgenommene äußere Umstände eingefordert werden, werden andererseits gerade angesichts der Tatsache, dass von Souveränität womöglich nurmehr metaphorisch die Rede ist, auch relativierende Relationen hervorgehoben: So lassen sich der Annahme einer vermeintlichen völligen Ungebundenheit des souveränen Subjekts dessen zwangsläufig bestehende, unvermeidbare Abhängigkeiten von seiner physischen wie sozialen Leiblichkeit entgegenhalten (vgl. Böhme 2008: 188). »Herren unserer selbst« sind wir schlechterdings nicht. Der Einsicht in die relevanten Beziehungsgeflechte noch des souveränen Subjekts korrespondiert zugleich eine stärkere Konzentration auf die Frage, wie mit unhintergehbaren Abhängigkeiten und Kompetenzbegrenzungen umzugehen ist. Das lenkt den Blick auf Mechanismen, die zwar nicht alle existierenden Bindungen zu lösen vermögen, aber doch geeignet sind, zumindest kontrollerhöhend zu wirken. Ersichtlich ist ein solches, zwangsläufig unvollständiges und lernendes Konzept eher imstande, neuere Schutzinstrumente zu integrieren und deren Verbesserungsfähigkeit zu berücksichtigen. Das deutet Unterschiede zwischen Staaten- und Daten-Souveränität an: An die Stelle eines illusorisch-absoluten, klassisch-philosophischen Traditionen verpflichteten Unabhängigkeitspostulats tritt ein stärker kontextorientiertes, aushandlungsbasiertes und graduelles Souveränitätsverständnis. Dessen Orientierung am menschlichen Körper markiert zugleich einen signifikanten Unterschied zum großenteils eigentumsanalog konstruierten Datenschutzrecht.

Der herkömmliche Datenschutzgedanke wird mit der hier vertretenen Sicht dennoch nicht aufgegeben, sondern weiterentwickelt, den Herausforderungen der Gegenwart angepasst und mit einem ebenso voraussetzungs- wie anspruchsvollen, eine Vielzahl von Akteuren einbindenden und innovationsoffenen Gestaltungs- und Regelungskonzept abgesichert. Eine solche komplexe Gewährleistungsdimension lässt sich nicht durch bloße Teilmodifikationen einzelner Instrumente oder gar allein durch zusätzliche

Ressourcenzuweisungen und erhöhte Durchsetzungskapazitäten sicherstellen. Sie verlangt eine weitreichende, rechtliche wie außerrechtliche Mechanismen einbeziehende gesamtgesellschaftliche Anstrengung. Es bedarf flexibler und problemadäquater, institutionell diversifizierter Regulierungsansätze. Zwei exemplarische Aspekte mögen dies verdeutlichen: Unter Big-Data-Bedingungen ist es erstens notwendig, sich von überholten Vorstellungen einer spezifischen, vorgegebenen Sensibilität bestimmter Daten und hierauf rekurrierender besonderer Schutzmechanismen zu lösen. Datenschutz kann nicht mehr statisch an bestimmten Daten und Datennutzungskategorien ansetzen, sondern muss sich auf ständige Rekombinationen und Rekontextualisierungen einstellen. Dabei genügt es zweitens nicht, an einigen wenigen Stellschrauben zu drehen. Vielmehr sind die diversen Beteiligten und Handlungskontexte und die vielfältigen Verantwortlichkeiten zu berücksichtigen. Diese Multiakteursverantwortung erfasst selbstverständlich auch die Datenverwender in Wirtschaft und Forschung. Die dort zentrierte Expertise ist von elementarer Bedeutung. Technologisch induzierte Probleme verlangen nach technologisch unterstützten, jedenfalls aber technologisch informierten Lösungen (Appenzeller u. a. 2021: 173 f.).

Datensouveränität bildet aber nicht nur einen Maßstab für Veränderungen im Verhältnis von Regulierern und Regulierten, sondern wer sich auf sie beruft, nimmt namentlich die Ausgangssubjekte der personenbezogenen Daten mit in den Blick. Sie müssen zu einem souveränen Umgang mit ihren Daten befähigt werden. Das entwickelt das bekannte Konzept der informationellen Selbstbestimmung in einer spezifischen Richtung weiter: Informationelle Freiheitsgestaltung meint interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt. Die Betonung des Freiheitsgedankens verdeutlicht, dass es nicht um ein an das Eigentumsgrundrecht angelehntes Ausschlussrecht geht. Stattdessen steht die Befugnis im Zentrum, selbst zu bestimmen, mit welchen Inhalten man in Beziehung zur Umwelt tritt. Entscheidend ist weniger die – ohnehin illusorische – jederzeitige Hoheit über die eigenen Daten als die Möglichkeit, verhaltenslenkendes, potenziell freiheitsbeschränkendes Verhalten erkennen und auf dieser Basis den Zugang zu Daten kontrollieren zu können. Ein solches Souveränitätsverständnis verklärt die Datengeber nicht zu vermeintlich gänzlich ungebundenen Subjekten, sondern berücksichtigt die situationsbedingten Abhängigkeiten und namentlich die mit Machtasymmetrien verbundenen Gefährdungen. Auf der Governanceebene verlangt

es neben informatorischen (dazu Krüger 2016: 190 f.) und edukatorischen Maßnahmen klare Regelungsvorgaben, so zum Beispiel Missbrauchs- und Diskriminierungsverbote. Darüber hinaus sind freiheitssichernde technische Unterstützungsmechanismen miteinzubeziehen. Ferner wird nicht verkannt, dass eine zunehmend datenbasiert funktionierende Gesellschaft auf qualitativ hochwertige, valide Daten angewiesen ist. Deshalb wird die Freiheits- um eine Verantwortungsperspektive ergänzt. Demnach ist im Rahmen der informationellen Freiheitsgestaltung (auch) geboten, sich an den gesellschaftlichen Anforderungen von Solidarität und Gerechtigkeit zu orientieren. Dies bedeutet zwar keineswegs eine Pflicht zur Preisgabe individueller Daten. Aber auch mit Blick auf den Schutz von Daten ist eine individuelle wie gesellschaftliche Verantwortung gegenüber Anderen, insbesondere in spezifisch hilfsbedürftigen und vulnerablen Positionen, zu berücksichtigen. Der Ausdruck »Verantwortung« besitzt im Digitalbereich indes nicht nur auf der Ebene der Individuen Bedeutung. Die Frage der Verantwortung betrifft auch Institutionen und insbesondere den Staat. Die Pflicht der Individuen, Verantwortung für die Nutzung der eigenen Daten zu übernehmen, setzt dementsprechend voraus, dass hierfür geeignete Rahmenbedingungen geschaffen werden. Einen möglichen Anwendungsfall für eine solche bewusste, aber auch begrenzte Öffnung stellt das jüngst wieder intensiv diskutierte Modell einer sogenannten Datenspende dar (vgl. Hummel u. a. 2019). Datensouveränität erschöpft sich nicht in der abwehrrechtlichen Dimension, obschon sie auch den Schutz von Persönlichkeitsrechten und Freiheitssicherung umfasst. Sie ist indes zugleich mit dem Anspruch verbunden, Daten verfügbar machen zu können (vgl. Hummel u. a. 2018). Insoweit verlangt sie, den Einzelnen in die Lage zu versetzen, beide Aspekte wahrzunehmen und zwischen ihnen abzuwägen. Um die entsprechende Kontrollierbarkeit sicherzustellen, wird eine Weiterentwicklung des klassischen Einwilligungsmodells in Richtung eines sogenannten Dynamic Consent vorgeschlagen (Hummel u. a. 2021a: 11 sowie Augsberg/von Ulmenstein 2018). Ausdruck der beabsichtigten kontrollierten Öffnung können darüber hinaus insbesondere Datentreuhänder sein (Hummel u. a. 2021a: 17 ff.; vgl. auch Bizer 1999; Kühling 2021; RfII 2020).

## 4. Data Governance: Daten als Wirtschaftsfaktor

Das schließt den Bogen zum dritten Leitprinzip. Dieses betrifft die Data Governance. Hierunter könnte man zunächst in einem weit gefassten Begriffsverständnis diejenigen Regeln und Rechte fassen, die in Bezug auf die Sammlung, Produktion, Verarbeitung, Analyse, Nutzung, Lizensierung bzw. den Verkauf von Daten eine Rolle spielen. In Anlehnung an die steuerungswissenschaftliche Forschung (siehe nur Benz 2010) ginge es demnach (nur) darum, unterschiedliche Steuerungsmaßnahmen auszuloten und namentlich rechtliche Instrumentarien sozialwissenschaftlich fundiert einzusetzen. Das eröffnete eine große Bandbreite an Optionen. Gerade deshalb ist aber zweifelhaft, ob mit einer derart allgemeinen Begriffsverwendung viel gewonnen wäre; jedenfalls dürfte sie schon aufgrund ihrer weitgehenden inhaltlichen Neutralität kaum tauglich sein, als zukunftsweisendes Leitprinzip für den Umgang mit Daten zu dienen. Stattdessen ist deshalb ein spezielleres Verständnis in den Blick zu nehmen, das dem Data Governance Act (DGA) der Europäischen Union zugrunde liegt und diesen prägt (vgl. zum Folgenden Spindler 2021b).

Der DGA bildet einen integralen Bestandteil der Strategie der Kommission zur Herstellung eines europäischen Datenwirtschaftsraums. Als sein Hauptziel gilt es, die Verfügbarkeit und den Austausch von Daten zu erleichtern. In dieser Perspektive stehen Daten folglich weniger in Parallele zum Privateigentum oder zum menschlichen Körper. Sie werden vielmehr als Gesellschafts- und Wirtschaftsfaktor betrachtet, der prinzipiell von einem erleichterten Zugang und Austausch profitiert. Zu diesem Zweck werden unterschiedliche, weitgehend unabhängig voneinander funktionierende Mechanismen eingeführt:

Erstens werden – in Fortschreibung der Open-Data-Strategie (vgl. Hartl/Ludin 2021) –Regelungen geschaffen, um die sichere Weiterverwendung von Daten des öffentlichen Sektors zu ermöglichen, auch wenn sie den Rechten anderer unterliegen. Da dies unter anderem auch personenbezogene Daten betrifft, bedarf es einer entsprechenden technischen Ausstattung, um einen adäquaten Schutz von Privatsphäre und Vertraulichkeit sicherzustellen. Zweitens wird der rechtliche Rahmen für das neue Geschäftsmodell der Datenvermittlung kreiert. Diese spezifischer Regulierung (Registrierung und freiwillige Zertifizierung) unterliegenden Datenintermediäre sollen ein sicheres Umfeld für den Datenaustausch bilden; das wird als kontrollverstärkende und missbrauchsvermeidende Maßnahme verstanden, die gleichzei-

tig die Menge der zur Verfügung stehenden Daten erhöht. Datenintermediäre dürfen für ihre Dienstleistungen Gebühren erheben. Es ist ihnen aber untersagt, die gemeinsam genutzten Daten für andere Zwecke zu verwenden, insbesondere, sie ökonomisch zu verwerten. Drittens enthält der DGA Bestimmungen zum sogenannten Datenaltruismus. Die Regelungen sollen es Einzelpersonen und Unternehmen erleichtern, ihre Daten freiwillig aus Gemeinwohlgründen zur Verfügung zu stellen (etwa zur Forschung). Im Interesse des Vertrauensschutzes sind auch insoweit entsprechende regulatorische Anforderungen (Registrierung und freiwillige Zertifizierung) für anerkannte datenaltruistische Organisationen vorgesehen.

## 5. (Zwischen-)Fazit: Tatendurst und Datenhunger

Auf Basis dieser kurzen, notwendig holzschnittartigen Beschreibungen wird deutlich, dass die unterschiedlichen Leitbegriffe unterschiedliche Zielsetzungen und Verfahrensanforderungen implizieren, gleichzeitig aber auch nicht unerhebliche Schnittmengen bestehen: Datenschutz und Datensouveränität eint etwa der Fokus auf Individuen und die multiplen Ebenen der Kontrolle bzw. Partizipation. Die Paradigmen unterscheiden sich indes in ihrem Fokus auf die negative und/oder positive Freiheit. Bei letzterer – der Idee einer Gestaltungs- und Verwendungsfreiheit im Hinblick auf Daten – kommt die Data Governance stärker ins Spiel. Verdeutlichen kann dies das Beispiel der Datenspende. Wie jüngst in der Diskussion über eine freiwillige Preisgabe der pandemiebezogenen (Kontakt-)Daten aus Warn-Apps wie auch manueller Erfassung wieder deutlich wurde, können Spender auf diese Weise – also durch bewusste Freigabe ihrer Daten für die wissenschaftliche Nutzung – wohltätig wirken, Solidarität üben und zugleich am wissenschaftlichen Fortschritt teilhaben. »Spenden« besitzen insoweit durchaus einen potenziell reziproken Charakter. Jedenfalls ist offensichtlich, dass das Spenden mit positiven Erlebnissen und Gefühlen verbunden sein kann. Ob bzw. unter welchen Voraussetzungen eine Datenspende indes derzeit datenschutzrechtlich zulässig ist, ist umstritten. Mit Blick auf die DSGVO bestehen einerseits Bedenken angesichts der grundsätzlich engen Zweckbindung. Andererseits enthält die DSGVO durchaus Anhaltspunkte für eine Auflockerung dieser Anforderungen, und speziell mit Blick auf die primär praxisrelevante Datenspende zu Forschungszwecken ist auf die entsprechende Privilegierung der Sekundär- und Tertiärnutzung hinzuweisen.

Deshalb spricht auch diesseits der Neuregelungen des europäischen DGA zum Datenaltruismus einiges dafür, hier keinen pauschalen Verstoß gegen geltendes Datenschutzrecht anzunehmen. Eine strenge, die Datengeber zu bloß passiven Schutzobjekten reduzierende Betrachtung, die Mitgestaltung womöglich sogar definitiv ausschließt, ist abzulehnen. Dass aber entsprechende Spannungen rechtlich wie politisch bestehen, verdeutlicht die bleibende Relevanz der unterschiedlichen Grundansätze: Man hält an »Schutz« wie auch an »Selbstbestimmung« fest.

Eine zweite exemplarische Überlegung mag dies weiter veranschaulichen: Ersichtlich besteht in allen Regulierungskonzepten ein Interesse daran, Methoden zu finden, mit denen die Kontrollfähigkeit der Datengeber erhöht werden kann. Allerdings unterscheiden sie sich hinsichtlich der Frage, ob in diesem Zusammenhang auch parallele (bewusste) Kontrollverluste oder entsprechende Modifikationen zulässig sind. Beispielsweise sind die Möglichkeiten, Entscheidungen unterschiedlich auszugestalten oder an Dritte abzugeben, im geltenden Datenschutzrecht wenig ausgeprägt. Das zeigt sich besonders deutlich an den Schwierigkeiten, flexibilisierende Elemente in das klassisch-starre Einwilligungsmodell zu inkorporieren. Auch das Konzept des Datentreuhänders gilt datenschutzrechtlich tendenziell als problematisch, soweit es zwar einerseits zusätzliche Steuerungs- und Gestaltungsoptionen beinhaltet, andererseits aber auch einen gewissen Verlust von (Eigen-)Kontrolle umfasst (dazu näher Hummel u. a. 2021a: 14 ff.; Kühling 2021; Specht-Riemenschneider u. a. 2021). Aus Sicht der Datensouveränität und der Data Governance lässt sich hingegen durch Datentreuhänder und andere Intermediäre eine sonst kaum mögliche oder zumindest schwer praktikable »controllability« erreichen. Der Kollektivierungsmechanismus erleichtert bzw. sichert damit individuelle Einflussnahmemöglichkeiten – damit bestehen auch Überschneidungen zur sogenannten »group privacy« und der auf diese Weise auf den Begriff gebrachten Schutzbedürftigkeit nicht nur individueller, sondern auch kollektiver Interessen.

Datentreuhandmodelle sind ferner aus Datensouveränitätsgründen auch deshalb attraktiv, weil das Treugut nicht auf (personenbezogene) Daten mit einem spezifischen Informationsgehalt beschränkt bleiben muss, sondern etwa auch – an sich datenschutzrechtlich kaum erfassbare, aber datenschutzrelevante – Korrelationsmuster einbeziehen könnte. Allerdings müssten hier Vorkehrungen getroffen werden, unkontrollierte und unkontrollierbare Ausweitungen zu verhindern. Um eine hinreichend kontextbezogene, transparenz- und qualitätssichernde Rechenschaft von

Analyseergebnissen zu ermöglichen, bietet sich deshalb die Verbindung von Datentreuhandkonzepten mit einem spezifischen Modell eines dynamisierten Einwilligungsmodells an. Ebenso sollten B2B-Beziehungen, also der Datenaustausch zwischen Unternehmen und überhaupt der Anspruch von Unternehmen, hinsichtlich ihrer Daten »souverän« zu sein, näher betrachtet werden. Das geht indes ersichtlich über die bislang im DGA vorgenommene Orientierung hinaus.

Insgesamt dürfte deutlich geworden sein, dass ein gemeinsames, hohes Interesse daran besteht, hinreichend viele und qualitativ hochwertige Daten zu erhalten und dauerhaft nutzen zu können, andererseits aber hierfür nicht den (zu) hohen Preis eines weitgehenden Kontrollverlusts zu bezahlen. Wenn Daten als »Rohstoff des 21. Jahrhunderts« zu verstehen sind, müssen Datennutzung und Datenschutz zusammen gedacht und regelungstechnisch miteinander verbunden werden (ähnlich Specht-Riemenschneider/Blankertz 2021). Das setzt unter anderem ein hohes (System-)Vertrauen der Datengeber voraus. Gerade im Kontext des in Deutschland notorisch sensiblen Themas Datenschutz bedarf es hierfür einer konzertierten und koordinierten Anstrengung, die nicht reflexhaft Änderungen ablehnt, aber vorhandene Erfahrungen im Sinne einer integrativen Anstrengung würdigt und nutzt. Ein im oben beschriebenen Sinne entwicklungsoffenes Leitbild »Datensouveränität« kann dazu beitragen, dieser regulatorischen Herausforderung Herr zu werden. Es umschreibt Grundlagen und Grenzen einer immer granulareren Datenerhebung, -analyse und -verwendung. Es garantiert dem Einzelnen die realistische Möglichkeit, in der digitalisierten Welt die eigene Identität zu bewahren und zu gestalten sowie die eigenen Handlungen vor sich und anderen zu verantworten. Auf dieser Basis sind nicht nur Abwehrmaßnahmen, sondern auch kontrollierte, gemeinwohlnützliche Datenaustauschvorgänge möglich.

# Zwischen Datensouveränität und Volkssouveränität: Demokratietheoretische Überlegungen mit und gegen Hannah Arendt

*Tim Eckes*

Datensouveränität ist spätestens seit Ende des Jahres 2015 als Konzept wie auch als Postulat in nahezu aller Munde: Vom damaligen Wirtschaftsminister Sigmar Gabriel zunächst öffentlichkeitswirksam und offensiv als Konkurrenz zum klassischen Datenschutz ins Spiel gebracht sowie in der Digitalen Strategie 2025 verankert (BMWi 2016), hat es das Konzept inzwischen in derart viele Publikationen, Aufsätze und Tagungen geschafft (siehe unlängst Beise/Eckes 2021), dass es in Sachen Aufmerksamkeit nahezu gleichauf zu sein scheint mit der ubiquitär diskutierten Idee der Digitalen Souveränität (siehe z. B. Friedrichsen/Bisa 2016; Floridi 2020; Pohle 2020a; Pohle/Thiel 2022).[1] Ungeachtet aller Differenzen zwischen den beiden Konzepten, der Datensouveränität einerseits, der Digitalen Souveränität andererseits,[2] ist das diskursive Terrain rund um das Thema Digitalisierung damit in einem Ausmaß durch eine Renaissance der Souveränität geprägt, dass sich unweigerlich ein Gefühl der Verblüffung einstellen muss – eine Verblüffung jedenfalls aus der spezifischen Perspektive einer Politischen Theorie und Philosophie, die in den letzten 25 Jahren kaum ein gutes Haar an der Souveränität gelassen hat und zuweilen gar bereit schien, diese Kategorie gleich ganz zu beerdigen. Dass jedoch Totgesagte länger leben, ist eine Binsenweisheit, die die neuerlichen Diskurse um Digitalisierung und die Rolle der Souveränität in ihnen geradezu vortrefflich zu charakterisieren scheint. Freilich: Die unerwartete Tatsache, dass die Souveränität inzwischen wieder höchst

---

1 Im Handbuch *Digitalisierung in Staat und Verwaltung* (Klenk/Nullmeier/Wewer 2020) hat allerdings nur die Digitale Souveränität einen eigenen Eintrag bekommen. Es ist dann auch nur im Rahmen dieses aus der Feder von Julia Pohle stammenden Eintrags, dass die Datensouveränität überhaupt erwähnt wird (vgl. Pohle 2020a: 245 ff.).

2 Vgl. den Beitrag von Gehring in diesem Band.

lebendig auf Erden zu wandeln scheint, hat nicht dazu geführt, dass sich die in den letzten Jahrzehnten innerhalb der Politischen Theorie eingeübte Skepsis gegenüber der Souveränität nun in Wohlgefallen aufgelöst hätte und sie mit offenen Armen auf dem diskursiven Feld der Digitalisierung empfangen würde. Im Gegenteil: Blickt man beispielsweise auf die Veröffentlichungen von Thorsten Thiel und Julia Pohle, dann ist Souveränität dort jeweils derart problematisch, dass sogar vor ihrer Wiederkehr gewarnt, ja regelrecht gemahnt werden muss: Souveränität verbinde sich, so durchgängig die Kritik, mit Hierarchie, Zentralismus, Nationalismus und gar Homogenität – mit Eigenschaften also, die mit dem robusten Pluralismus gegenwärtiger demokratischer Gesellschaften kaum zu vereinbaren seien (vgl. vor allem Thiel 2021; Pohle/Thiel 2021: 321, 337 ff.; vgl. zur Volkssouveränität auch Thiel 2019: 55, Fn. 6). Zwar ist diese Kritik speziell auf die Digitale Souveränität bezogen,[3] doch ist sie jeweils derart generalisierend vorgetragen, dass kaum Zweifel daran aufkommen können, dass sie sich auf die Souveränität an sich und daher auch auf ihre unterschiedlichen Spielarten, das heißt auch auf die Datensouveränität bezieht. Just dies könnte wiederum ein Grund dafür sein, dass selbst der mit einiger Emphase vorgetragene Rückgriff auf die Souveränitätskategorie auf dem Feld der Datensouveränität von einer merkwürdigen Zurückhaltung umgeben scheint: So entwickelt der Deutsche Ethikrat in seiner Stellungnahme aus dem Jahr 2017 (Deutscher Ethikrat 2018) zwar auf über 300 Seiten ein Konzept der Datensouveränität, das die Ebene des Individuums mit der des Sozialen verbindet, doch wenn sogleich klargestellt wird, dass »[d]er Einzelne […] maßgeblicher Bezugspunkt von Datensouveränität [bleibt]« (Deutscher Ethikrat 2018: 253), dann ist die Souveränität der Datensouveränität trotz aller Betonung der »kollektiven Dimension« (ebd.) von Daten letztlich doch beim Individuum monopolisiert. An das heiße Eisen einer demokratischen Volkssouveränität auf dem Feld der Digitalisierung wollte sich auch der Ethikrat scheinbar gar nicht erst wagen[4] – dies eine Aussparung jedoch, die nicht nur demokratietheoretischen Argwohn gera-

3 Ohnehin kommt die Datensouveränität bei Pohle/Thiel kaum vor (siehe jedoch, wie bereits erwähnt, Pohle 2020a: 245 ff.); vgl. auch den Beitrag von Gehring in diesem Band.

4 Vor diesem Hintergrund überrascht es dann auch nicht, dass die Demokratie in der Stellungnahme des Ethikrates auch insgesamt eher eine randständige Rolle spielt und nur im Kontext »des demokratischen Verfassungsstaates« (Deutscher Ethikrat 2018: 157) überhaupt einmal erwähnt wird – dies eine bemerkenswerte Bilanz für ein Dokument, das sich auch in die Untiefen der politischen Philosophie vorwagt und Autoren wie Rawls und Rorty zitiert (vgl. zu Rawls Deutscher Ethikrat 2018: 187, Fn. 282; zu Rorty Deutscher Ethikrat 2018: 230, Fn. 348).

dezu provozieren muss, sondern auch allerlei offene Flanken für expertokratischen Zugriff, ja womöglich gar für die Entstehung einer datenbezogenen »Gerechtigkeitsexpertokratie« (Maus 2011: 86) enthält.

Nun ist der in der Politischen Theorie zu beobachtende Argwohn gegenüber der Souveränität freilich nicht grundlos, sondern hat diverse empirische und theoretisch-ideengeschichtliche Gründe. Was dabei zunächst die empirische Dimension betrifft, so schien die Idee der Souveränität mit dem Prozess der europäischen Integration, aber auch mit diversen globalen Rechtsentwicklungen (z. B. im Rahmen der UN) in der Praxis regelrecht obsolet zu werden, während zugleich die rasante technische Entwicklung des Internets die Skepsis gegenüber der Souveränität zunächst noch zu untermauen schien (so jedenfalls die anarchisch-libertäre Anfangsdeutung dieser Entwicklung). Auf der politiktheoretischen Ebene wurde dieser Prozess wiederum durch eine Diskurslandschaft begleitet, die sich auf Themen wie Kosmopolitismus und universelle Menschenrechte konzentrierte, dann jedoch fast gänzlich im Zeichen des kometenhaften Aufstiegs der politischen Philosophie Hannah Arendts stand. Deren Werk konnte zwar kaum etwas Positives zu den Kosmopolitismus- und Menschenrechtsdebatten dieser Zeit beitragen, es enthält jedoch eine harsche, fast schon kompromisslose Souveränitätskritik, die über die verschiedenen Rezeptionsbahnen bis tief in den aktuellen Diskurs zur Digitalisierung nachhallt und geradezu als Blaupause für die oben angesprochene Souveränitätskritik beispielsweise von Thorsten Thiel betrachtet werden kann.[5] Selbst wo Arendt im aktuellen kritischen Digitalisierungsdiskurs also nicht explizit bemüht wird, ist sie dennoch eigentümlich präsent.

Die folgenden Überlegungen beruhen nun auf der Annahme, dass die Präsenz der Arendt'schen Souveränitätskritik im Digitalisierungsdiskurs ihrerseits zu kritisieren ist. Im Folgenden soll daher eine Kritik der Souveränitätskritik versucht werden, deren leitende Annahme darin besteht, dass diese Kritik, welche Formen von Souveränität sie auch immer zu treffen vermag, die moderne Version der an Kant und Rousseau anschließenden Theorie der Volkssouveränität jedoch kaum trifft, sondern diese eher gründ-

5 Was Thorsten Thiel selbst angeht, so hat sich dieser vor allem im Rahmen seiner lesenswerten und thematisch einschlägigen Dissertation *Republikanismus und die Europäische Union* (Thiel 2012) sowie in einigen Aufsätzen mit Hannah Arendt beschäftigt; vgl. Thiel 2013, 2014.

lich missversteht.[6] Diese Theorie – ist sie erst einmal gegen Arendts Kritik verteidigt – könnte also durchaus als demokratietheoretischer Bündnispartner der Datensouveränität auftreten. Zugleich darf dieser insgesamt Arendt-kritische Befund allerdings nicht als Verabschiedung Arendts oder als Warnung vor einer »Arendt-Falle« (Jörke 2016: 201) gedeutet werden: Denn nicht nur kann Arendt in einer sehr eng umgrenzten Hinsicht ein interessantes Problem identifizieren, von dem auch die Theorie der Volkssouveränität partiell betroffen ist – das Risiko einer überschießenden Moral nämlich –, sondern auch einige Theorieelemente liefern, die sowohl das Konzept der Datensouveränität konstruktiv weiterentwickeln können als auch die Idee der Datengenossenschaft demokratietheoretisch zu konturieren vermögen.

## 1. Hannah Arendts (Miss-)Verständnis von Souveränität

Hannah Arendt hat eine Kritik der Souveränität an den verschiedenen Stellen ihres weitläufigen Werkes in unterschiedlichsten Varianten ausformuliert. Möchte man eine möglichst knappe Zusammenfassung des Inhalts dieser Kritik, dann bietet sich zunächst wohl Jean Cohens konzise formulierter Hinweis darauf an, Arendt verstehe Souveränität als »assertion of the will, command, and ultimate discretion of an uncommanded commander who is *legibus solutus*« (Cohen 2007: 299), und zudem als »arbitrary, hierarchical, levelling, homogenizing, and solipsistic by definition« (ebd.). Wollte man für diese knappe Erläuterung drei Schlagworte ausfindig machen, dann wären dies also wohl: Hierarchie, Homogenität und Willkür. Oder um es mittels Negationen zu sagen: Souveränität ist in der Arendt'schen Theoriesprache antipolitisch, anti-pluralistisch und anti-weltlich. Folglich scheint sich in Begriff und Empirie der Souveränität für Arendt nahezu undifferenziert alles Verdammungswürdige zu konzentrieren. Die folgenden Ausführungen sollen

6 Wenn im vorliegenden Aufsatz von Volkssouveränität und der zugehörigen Theorie die Rede ist, dann ist diese stets im Sinne eines »Kantischen Republikanismus« (Niesen 2001: 569) zu verstehen. Diese Theoriefamilie oder -richtung hat sich immer wieder offensiv von konkurrierenden Interpretationen der Volkssouveränität, allen voran derjenigen Carl Schmitts, abgegrenzt (vgl. zur Kritik schon Maus 1980). Diese Abgrenzung hält sich nicht zuletzt auch in dem alternativen, spezifisch rechtstheoretischen Label durch, das sich für diese Theorie findet: Demokratischer Positivismus (so Niesen/Eberl [2]2009).

jedoch zeigen: Der differenzierende Blick lohnt sich durchaus – auch wenn die drei Aspekte eng und bei Arendt in der Tat fast bis zur Verschmelzung miteinander verbunden sind.

Unter dem erstgenannten Gesichtspunkt der Hierarchie hält Arendt zunächst eine herrschaftstheoretische Problematik fest, die von ihr dann auch normtypologisch ausbuchstabiert wird. Seine womöglich prägnanteste Ausformulierung findet dieser Gesichtspunkt in Arendts Hauptwerk *Vita activa*, wo sie im Kontext von Platons *Politikos* eine aus ihrer Sicht deformierte Vorstellung politischen Handelns erläutert, die darauf ziele, »eine Möglichkeit zu gewinnen, den Führer und Anfänger auch Herr seiner Aktion bleiben zu lassen in *souveräner* Unabhängigkeit von denen, ohne die er ja eigentlich seine Tat nicht vollenden kann« (Arendt 2002: 281, meine Hervorhebung, TE). Während Arendts eigener Begriff des Handelns umgekehrt bekanntlich mit aller Emphase darauf beruht, dass Einzelne jeweils etwas Neues beginnen und andere ihnen dann »*freiwillig* zu Hilfe kommen oder einem Unternehmen sich anschließen werden« (ebd., meine Hervorhebung, TE) – was ersichtlich mit Überzeugungsarbeit und dem Risiko des Scheiterns verbunden ist –, ist die hier mit Souveränität identifizierte Unabhängigkeit Arendt zufolge nur möglich, »wenn man […] über andere so verfügen kann, dass sie […] nicht handeln, sondern Befehle ausführen« (ebd.). Dem damit ins Spiel gebrachten Normtyp des nicht mit Freiwilligkeit, sondern vielmehr mit hierarchischem Zwang verbundenen Befehls verleiht Arendt in *Über die Revolution* dann auch zugleich einen religiösen Charakter, wenn sie von Gesetzen im Sinne der »Gebote Gottes [spricht, TE], in denen dem Menschen *von außen* gesagt wird: Du sollst! Oder: Du sollst nicht!« (Arendt 2011a: 244, meine Hervorhebung, TE) Dieser Verweis auf das absolute, einem göttlichen Sollen gleiche Außen ist interessant, weil er zugleich verdeutlicht, dass befehlende Subjekte aus Arendts Sicht keineswegs zu Oberhäuptern einer stabilen innerweltlichen Herrschaftsbeziehung werden, sondern vielmehr aus aller weltlichen Relationalität überhaupt herausfallen: Die anvisierte »souveräne« Unabhängigkeit gewinnen sie bei Arendt eben nur um den Preis des gleichzeitigen Verlusts sämtlicher Beziehungen – und just dieser Verlust resultiert wiederum aus dem Bruch mit dem »sozial-ontologischen Kontinuum« (Brunkhorst 1999: 143), der für das Mensch-Gott-Verhältnis charakteristisch sein mag, für zwischenmenschliche Relation jedoch, so eine und vielleicht auch nicht die unwichtigste Pointe von Arendts Philosophie, geradezu ruinös wirkt.

Unternimmt man nun den Versuch, diese Konzeptualisierung von Souveränität in ein Verhältnis zur modernen, speziell an den Kantischen Republikanismus anknüpfenden Idee der demokratischen Volkssouveränität zu setzen, dann lässt sich mit Blick auf die Übersetzung von Souveränität in Unabhängigkeit und von dieser in den metaphysisch-exekutivischen Befehl umstandslos ein recht klarer Befund ziehen: Arendts Kritik richtet sich gar nicht auf den begrifflich-konzeptuellen Ideal- oder Normalfall von (Volks-)Souveränität, sondern vielmehr auf deren Deformation. Aus dem Kreis der verschiedenen Theoretikerinnen der Volkssouveränität hat vor allem Ingeborg Maus immer wieder vehement und sehr zu Recht darauf verwiesen, dass Souveränität sowohl bei Rousseau als auch bei Kant vollständig deckungsgleich sei mit der legislativen Gewalt und die Allokation ebendieser Gewalt beim Volk wiederum das ganze Kernprinzip der Volkssouveränität ausmacht:

»Das Prinzip der Volkssouveränität, wie es im 18. Jahrhundert entwickelt wurde, enthält [...] eine normative Aussage über die Allokation politischer Macht. [...] Souveränität ist (in langer ideengeschichtlicher Tradition) identisch mit der Funktion der Gesetzgebung.« (Maus 2011: 367 f.)

Steht damit gerade nicht der exekutiv-hierarchische Befehl, sondern das allgemeine und gleiche Gesetz für Souveränität, so führt Maus speziell mit Blick auf die rechtsstaatlichen Implikationen der Volkssouveränität aus, dass »dem Volk (oder seinen Vertretern im Gesetzgebungsorgan) alle, aber auch nur die Gesetzgebung zukommt«, weshalb »die Gewaltenteilung durchgängig funktional bestimmt [wird]: Die ungeteilte Souveränität der Gesetzgebung findet ihre ›Grenze‹ an dem Verbot individueller Regelungen, welch letztere ausschließlich in die Kompetenz der anwendenden Apparate (Exekutive und Justiz) fallen.« (Ebd.) In der Tat: Einerseits ist die Theorie der Volkssouveränität bereits bei Rousseau und Kant derart rigoros gewaltenteilig-funktional abgesichert, dass das Gesetz zum prototypischen Anderen, gar zum Gegenspieler des exekutiven Befehls wird und mithin beide das Modell der Identität von exekutivem Befehl und Souveränität, das Arendt in ihrer Kritik als Normalfall unterstellt, in Form der griechischen polis sogar als Despotie betrachten (vgl. Eberl/Niesen 2011: 218 f.). Andererseits sind Rousseau und Kant gegenüber Fragen der personellen Gewaltenteilung aus systematischen Gründen zugleich derart desinteressiert und nicht-rigoros (vgl. Eckes 2011), dass der von Arendt im Außen lokalisierte Befehlshaber sogar – und in deutlichstem Gegensatz zum amerikanischen Modell der

*checks and balances* – in die Innenwelt der parlamentarischen Legislative vordringen und sich dort an der souveränen Gesetzgebung beteiligen darf. Kurzum: Arendt verfehlt nicht nur recht deutlich die mit der Volkssouveränität verbundene Dimension der funktionalen Gewaltenteilung – und mit ihr freilich all jene, die Souveränität in toto mit einer exekutiv geprägten »*Durchsetzungs*macht« (Pohle/Thiel 2021: 338, meine Hervorhebung, TE) kurzschließen –, sondern vor allem auch die personelle Komponente, die sich mit dem Prinzip der Volkssouveränität ebenso verbindet; und all dies wiederum, obwohl Arendt Kant andernorts zugleich explizit dafür lobt, die Bedeutung der Gewaltenteilung erkannt zu haben (vgl. Arendt 2007: 722). Man ist fast versucht zu sagen: Arendt trägt damit ein zutreffendes Lob aus den völlig falschen Gründen vor.[7]

Während Arendt die Theorie der Volkssouveränität speziell unter dem Aspekt der Hierarchie also kaum zu treffen vermag, lohnt im nächsten Schritt gleichwohl der Blick auf die gesellschaftstheoretische Dimension, die regelmäßig mit dem Schlagwort der Homogenität verbunden ist. Bereits in dem Aufsatz *Freiheit und Politik* hatte Arendt mit Blick auf diesen Zusammenhang bestimmt, dass »die Souveränität des einzelnen [wie] letztlich auch die Souveränität einer Gruppe oder eines politischen Körpers immer nur ein Schein [ist]«, der »nur dadurch zustande kommen [kann], dass eine Vielheit sich so verhält, als ob sie einer wäre und noch dazu ein einziger.« (Arendt 1994: 214 f.) Und Arendt ergänzt sogleich, dass »[s]olch ein Verhalten […] allerdings möglich [ist], wie wir aus vielen Phänomenen der Massengesellschaft nur zu gut wissen […]« (ebd.). Diese anti-pluralistische »Konstruktion einer vielköpfigen Einheit« (Arendt 2011a: 97) tritt dann auch in *Über die Revolution* prominent auf, wo Arendt mit dem an der französischen Revolution abgelesenen Bild einer Menge befasst ist, »›die in einem

7 Dies zeigt sich nicht zuletzt daran, dass Arendts Missverständnis im Kant-Lob selbst enthalten ist. So fügt sie im Zusammenhang mit der Gewaltenteilung in Klammern die Erläuterung hinzu: »which only Kant rightly understood as the decisive criterion of truly republican government and which only in the constitution of the American Republic found an adequate realization« (Arendt 2007: 722). Kant selbst dürfte das amerikanische Schema der Gewaltenteilung jedoch kaum als Realisierung seines eigenen funktional-vertikalen Konzepts verstanden haben. – So oder so sind diese Ausdeutungsversuche interessant. Denn heute gewinnt im Kontext digitaler Treuhandkonzepte die klassische Unterscheidung zwischen horizontal orientierten (*checks and balances*) und eher funktional-vertikal geprägten Gewaltenteilungsmodellen ganz neue Relevanz – und dies vor allem auch dann, wenn die beiden Modelle vermischt werden, wie z. B. bei Staab/Piétron 2021: 204.

Körper vereint‹ und von einem Willen beseelt ist, [...]; denn diese Menge war von Hunger getrieben, und der Schrei nach Brot ist unisono. Was den Hunger betrifft, gibt es keine Unterschiede« (ebd.: 120). Mehrmals identifiziert Arendt auf diese Weise die als homogenisierend ausgedeutete Dimension des Materiellen mit dem Sozialen und dieses Soziale dann wiederum mit der Volkssouveränität – dies eine in kritischer Absicht vorgenommene Gleichsetzung, die aus Sicht der bei Kant und Rousseau anschließenden, im Werk u. a. von Jürgen Habermas und auch Ingeborg Maus ausdifferenzierten Theorie der Volkssouveränität jedoch einige Verwunderung auslösen muss: Denn nicht nur ließe sich leicht argumentieren, dass die politische Philosophie mit den an der Idee der Volkssouveränität orientierten Theorien von Kant, Habermas und Maus über eine höchst avancierte Verteidigung von Pluralität verfügt, sodass hier von Homogenität oder auch »Einheitlichkeit« (Pohle/Thiel 2021: 338) eigentlich kaum noch etwas übrig bleibt. Es muss sich zudem auch – und gleichsam noch früher, weil methodisch ansetzend – Verwunderung einstellen angesichts der bei Arendt offensichtlich unterstellten These, dass die Theorie der Volkssouveränität selbst bereits eine Gesellschaftstheorie *ist*. Unnötig wären mit dieser Unterstellung u. a. die in der deutschsprachigen politischen Theorie langwierig geführten Debatten um die Begründung des Sozialstaats bei Kant (vgl. z. B. Thiele 2008: 157–169; Maus 1994: 167 ff.; kritisch Kersting $^{3}$2007: 264 Fn. 27, 33), überflüssig wäre auch die enorme intellektuelle Energie, die Habermas nicht nur für die Begründung, sondern auch für die scharfe Kritik des Sozialstaats im Lichte des Kolonialisierungstheorems investiert hat (vgl. Habermas 1995: 452, 531 ff.; vgl. Iser 2009), und schließlich würde auch die einfache Tatsache übergangen, dass eine mit der Volkssouveränität kompatible Vorstellung sozialer Demokratie bzw. des Sozialen ein nach wie vor laufendes Theorieprojekt ist, das immer noch einiger theoretischer Anstrengungen bedarf (vgl. Eberl/Salomon 2017).[8] Der Grund für all dies liegt letztlich darin, dass die Theorie der Volkssouveränität entschieden und durchaus auch rigide an der Trennung von Staat und Gesellschaft wie auch an der disziplinären Se-

8 Oliver Eberl und David Salomon sprechen in der Einleitung zu ihrem Band dann auch treffend von der »Aufgabe sozialer Demokratietheorie« (Eberl/Salomon 2017: 10), die sich im Kern daraus ergibt, das Prinzip der Volkssouveränität unter den Bedingungen der Postdemokratie neu zu denken und zu verwirklichen. Vgl. zum Theorem der Postdemokratie ursprünglich Crouch 2008.

parierung von Demokratietheorie und Soziologie festhält.[9] Und das würde eben auch Arendt zugeben müssen: Das Volk der Volkssouveränität ist in einem ganz emphatischen Sinne nicht deckungsgleich mit der empirischen ›Gesellschaft‹ oder einer der in ihr vorhandenen Gruppen – es ist eben keine soziale, sondern eine normativ-rechtstheoretische Größe.[10]

Stellt sich damit nach der herrschaftstheoretisch orientierten Kritik an Arendt auch die spezifisch gesellschaftstheoretische Kritik als eine Intervention dar, die die Theorie der Volkssouveränität keineswegs trifft, sondern vielmehr missversteht, so verhält es sich mit derjenigen Kritik anders, die Arendt ebenfalls vor allem in *Über die Revolution* vorträgt und die sich zugespitzt als moraltheoretische Dimension charakterisieren ließe. Im Zuge der dort auftauchenden Kontrastierung von »Volkswille« und geschriebener Verfassung bestimmt Arendt, dass die Verfassung »niemals ein […] ephemerer Gemütszustand sein konnte wie der sogenannte Volkswille« (Arendt 2011a: 204), der sich zudem »von Tag zu Tag, ja von Minute zu Minute ändert« (ebd.: 212). Was zunächst wie eine klassische Willkür- bzw. Voluntarismus-Kritik klingen mag, erhält durch den expliziten Hinweis auf den inneren »Gemütszustand« einen präzisen Sinn: Die von Arendt konstatierte Instabilität des souveränen »Volkswillens« resultiert nämlich keineswegs daraus, dass sich der Wille ständig neu äußern würde – wie man ja vermuten könnte –, sondern im Gegenteil aus der Abwesenheit jeder Äußerung, Externalisierung und damit Objektivierung überhaupt. Genau dieser Mangel an einer der objektiven Konsolidierung fähigen Äußerung ist es dann auch, den Arendt als Kernelement von Emotionen, Gemütszuständen und schließlich vor allem auch identifiziert mit: der Welt der Moral.[11] Entdeckt sich der »sogenannte Volkswille« bei Arendt folglich als primär moralisches Konstrukt, das mangels Objektivierung überhaupt nur

9 Das deutliche Festhalten an genau dieser Trennung erklärt dann auch viele weitere theoretische Abgrenzungen, darunter z. B. die Unterschiede zwischen dem Kantischen Republikanismus und den diversen Spielarten eines Zivilrepublikanismus.

10 Genau dies markiert im Übrigen auch eine wichtige Differenz zwischen allen populistischen Spielarten ›des Volkes‹ und dem Diskurs der Volkssouveränität. Dabei kommt neben den von diesem Diskurs stets betonten liberal-rechtsstaatlichen Elementen auch die zentrale Rolle demokratischer Prozeduren hinzu, die einen substanziellen demokratischen Willen nicht voraussetzen, sondern allererst erarbeiten helfen. Just diese Rolle von Prozeduren wird von Populisten regelmäßig ignoriert, wenn angenommen wird, dass der Wille des Volkes schon ›gegeben‹ oder irgendwie verfahrenslos zu ermitteln sei.

11 Nur folgerichtig ist es dann auch, dass sich Arendt in der Debatte um den zivilen Ungehorsam der Vorstellung eines innerlich-subjektiv bleibenden »*moralischen* Appell[s] an das Gewissen« (Celika-

per Zuschreibung existieren kann, so ist mit Blick auf den darin festgehaltenen Defekt der Volkssouveränität nun kaum von der Hand zu weisen, dass Arendt nicht nur die innerlich-monologische Struktur zumindest der Kantischen Moral treffend beschreibt,[12] sondern auch ein durchaus relevantes Problem der Volkssouveränität selbst identifiziert: Sah sich schon Kant aus guten Gründen genötigt, in *Zum ewigen Frieden* mit dem maximal moralfreien Grenzfall eines »Volks von Teufeln« zu operieren (vgl. Kant 1795, ²1796: 223 f., vgl. dazu Niesen 2001), so wurde umgekehrt Jürgen Habermas schon früh mit dem Vorwurf konfrontiert, dass das von ihm in *Faktizität und Geltung* konzipierte Verfahren der Rechtssetzung »die Bedingungen institutionalisieren [soll], unter denen *moralische* Argumente sich entfalten können« (Maus 2011: 275, meine Hervorhebung, TE). Bei Habermas sähen sich die Bürger, so unterstreicht Ingeborg Maus (ebd.), konfrontiert mit den durchaus moralischen »Erwartungen der Gemeinwohlorientierung« (Habermas 1998: 111). Trotz aller Modifikationen am Kantischen Grundgerüst bleiben Moral und Ethik für die Theorie der Volkssouveränität (wie auch für die politische Theorie insgesamt)[13] also nach wie vor ein felsiges Terrain, das von Arendt tatsächlich treffsicher vermessen wird. Freilich: Dass auch die mit der Volkssouveränität assoziierten Autor*innen diese kritische Vermessung auch selbst vorgenommen haben,[14] ist nicht nur ein Verweis auf das Problembewusstsein dieser Theorie selbst, sondern macht auch deutlich, dass Arendt hier kaum ein Copyright für sich beanspruchen kann. Von daher stellt sich jedoch umso dringender die Frage, ob sich in

---

tes 2017: 35, meine Hervorhebung, TE) nach dem Vorbild Thoreaus nicht anzuschließen vermag. Der gesamte Bereich der Moral bleibt für Arendt einer stabilen Objektivierung unfähig.

12 Vgl. hierzu auch die ähnliche Charakterisierung bei Ingeborg Maus, die mit Blick auf Kant darauf hinweist, dass das moralische »Prüfungsverfahren selbst […] eine monologische Struktur [hat] und […] *in foro interno* inszeniert [wird]« (Maus 1994: 330, meine Hervorhebung, TE).

13 Vgl. Jörke/Selk 2015; Jörke 2017. Freilich legen Jörke und Selk dabei zugleich großen Wert auf die Unterscheidung zwischen Moralisierung und Moral bzw. moralisch motivierter Kritik und sehen die Moralisierung vor allem als problematische Form eines Reduktionismus (vgl. Jörke/Selk 2015: 485, Fn. 6).

14 Eine ganz ähnliche Kritik wie Ingeborg Maus hat nämlich auch Peter Niesen formuliert. Dieser hat darauf hingewiesen, dass innerhalb der von Habermas vorgenommenen Differenzierung zwischen pragmatischen, moralischen und ethischen Diskursen keineswegs das Prinzip der Neutralität vorherrsche. Vielmehr habe Habermas das Bild einer »Gründehierarchie« (Niesen 2002: 44) entwickelt, »in der moralische Argumente […] andere Argumenttypen ›stechen‹ und als ›Trümpfe‹ fungieren« (ebd.: 44 f., vgl. auch Niesen/Eberl ²2009: 5). Damit steht die Moral bei Habermas gewissermaßen an der Spitze einer Pyramide, die bei fortgesetztem Dissens erreicht wird.

Arendts Theoriearsenal nicht Elemente auffinden lassen, die jenseits der bloßen Problemidentifikation auch eine konstruktive Weiterarbeit ermöglichen können. Die folgenden Ausführungen beruhen auf der Annahme, dass es genau diese Elemente bei Arendt gibt.

## 2. Hannah Arendts politische Philosophie – drei Differenzierungen

Hannah Arendts Souveränitätskritik strahlt – davon war ich ausgegangen – weit in den zeitgenössischen Digitalisierungsdiskurs aus. Dabei ist diese Kritik in ihrer sachlichen Reichweite durchaus begrenzt: Welche vor- oder auch post-modernen Theorien der Souveränität eine nach Arendt'schem Vorbild angelegte Souveränitätskritik auch immer zu treffen vermag, die an den Kantischen Republikanismus anschließende Theorie der demokratischen Volkssouveränität trifft sie jedenfalls kaum. Insofern drängt sich die Theorie der Volkssouveränität als konzeptueller demokratietheoretischer Partner für die im Digitalisierungsdiskurs verorteten Rückgriffe auf Souveränität und damit eben vor allem auch: für das Konzept der Datensouveränität geradezu auf. Folglich ließe sich das Konzept der Datensouveränität auch als Souveränität »von unten« auffassen und hierbei auf einen demokratietheoretischen Unterbau zurückgreifen, den es längst gibt. Allerdings haben die Überlegungen des letzten Abschnitts auch gezeigt, dass die Allianz aus Daten- und Volkssouveränität vorbeugend einer gewissen Modifikation bedürfte. In dem Maße nämlich, in dem Arendt mit dem Hinweis auf eine überschießende Moral ein durchaus relevantes Problem identifizieren konnte, rückt die Frage nach denjenigen Theorieelementen in den Fokus, die diesen Überschuss zwar nicht völlig ausschalten – dies wird ohnehin kaum das Ziel sein können –, aber kontrollierbar halten könnten, indem sie dem mit der Moral oftmals verbundenen Fokus auf das Innere und starke Normativität einen Fokus auf das Äußere und auch auf partielle Moralfreiheit entgegenstellen. Die folgenden Überlegungen zielen genau in diese Richtung. Sie beruhen auf der These, dass es in der Tat Arendt selbst ist, die solche Theoriestücke zu liefern vermag; diese sollen im Folgenden aus heuristischen Gründen entlang der Ebenen von Objekt, Subjekt und Intersubjektivität ausbuchstabiert und im nächsten Schritt auf das Konzept der Datensouveränität und vor allem die Idee der Datengenossenschaft über-

tragen werden. Im Übrigen wird dabei einer urteilstheoretischen Semantik gefolgt; dies zum einen wiederum aus heuristischen Gründen, zum anderen auf Grund der mitlaufenden Annahme, dass die folgenden Gesichtspunkte wichtige und bis dato noch kaum beleuchtete Implikationen für Arendts berühmtes Theoriestück der reflektierenden Urteilskraft enthalten. Aus Platzgründen werden diese Implikationen freilich an anderer Stelle weiter auszuführen sein.

Was nun zunächst die erste Ebene betrifft – also die Ebene dessen, was man als Objekt eines demokratisch reflektierten Urteilsprozesses beschreiben könnte –, so stellt sich die auf den ersten Blick recht einfache Frage danach, was eigentlich beurteilt wird. Tatsächlich ist mit dieser passiv ausgerichteten Formulierung, eben just der Frage danach, was beurteilt wird, bereits die eigentliche Crux angesprochen, denn das zwischen und vor den Urteilenden angesiedelte Objekt ist – in politischen Kontexten, in denen es wie auch immer indirekt um demokratische Selbstbestimmung geht – eben keineswegs so passiv, wie es die Fragestellung zunächst anzeigen mag. Deutlich wird dies, wenn sich der Blick auf die Frage richtet, was Arendt eigentlich unter einer Entität versteht, die in ihrer Philosophie immer wieder und durchaus auch prominent auftaucht: der Raum. Weit davon entfernt, zur Erläuterung ebendieses Konzepts die intuitive Vorstellung eines leeren Containers oder eines Vakuums zu bemühen,[15] ruft Arendt in *Vita activa* vielmehr die Metapher des Tisches auf (vgl. Arendt 2002: 66) und in *Was ist Politik?* dann sogar die paradoxe, weil den Raum direkt zum aktiven Subjekt erklärende Formulierung, wonach dieser als »Versamm*ler* von Menschen« (Arendt 2003: 64, meine Hervorhebung, TE) fungiere. Damit wird die landläufige Vorstellung von aktiver Subjektivität und passiver Dinglichkeit umgedreht: Denn nicht mehr treten aktive Subjekte »in« einen Raum und werden dort tätig, sondern umgekehrt ziehen die zwischen den Subjekten positionierten Dinge – in *Vita activa* eben: ein Tisch – die Subjekte aktiv an und bringen sie dazu, sich zu

15 Für Arendt bildet der »freie« Raum keinen neutralen Ausgangspunkt, sondern eher ein normatives und logisches Problem. Genau dies wiederum mag übrigens den interessanten und auch von Anna Jurkevics bemerkten Umstand erklären, dass Arendt in ihrem Exemplar von Carl Schmitts *Nomos der Erde* immer wieder den Ausdruck »freier Raum« markiert hat: »Arendt shows alarm and takes note wherever Schmitt says ›freier Raum‹, marking the margins with exclamations.« (Jurkevics 2017: 353) Während Jurkevics hier jedoch ein imperialismuskritisches Motiv vermutet, lässt sich Arendts Verwunderung auch schlichtweg darauf zurückführen, dass der freie Raum für sie ein Oxymoron ist: Aus ihrer Sicht ist ein Raum per definitionem mit Objekten gefüllt und kann daher niemals »frei« oder »leer« sein.

versammeln, in eine Beziehung zueinander zu treten und also zu einer Versammlung zu werden. Nicht nur lässt sich mit Blick auf Arendt so die These wagen, dass die zwischen den Subjekten positionierten Dinge bereits fertig konstituierte Subjekte bloß versammeln. Vielmehr bringen Objekte diese Subjekte unter Umständen allererst hervor und konstituieren diese sogar; und dieser Befund wiederum ist keineswegs so extravagant, wie es zunächst scheinen mag. Die Idee nämlich, dass Subjekte empirisch allererst post festum entstehen – reflektiv urteilende genauso wie souverän sich selbst bestimmende, rechtliche genauso wie politische und schließlich individualistisch geprägte ebenso wie kollektive –, ist ein in dieser Rolle bis dato leider noch kaum beleuchtetes[16] theoretisch-konstruktivistisches Bindeglied zwischen Arendts Theoriestück der (reflektierenden) Urteilskraft und der Theorie der Volkssouveränität.[17]

Richtet man den Blick nun auf die in den vorherigen Ausführungen freilich bereits implizierte Ebene der Subjekte, dann tritt vor allem eine Metapher in den Vordergrund, die in *Über die Revolution* prominent auftaucht: die Maske (vgl. Arendt 2011a: 135 f.). Diese von Arendt aufgerufene Metapher hat in der Sekundärliteratur leider ebenfalls bisher kaum größere Aufmerksamkeit auf sich gezogen.[18] Dies ist nicht nur deshalb misslich, weil Arendt dieses Motiv in den verschiedenen Werken wiederholt aufgreift, sondern auch,

16 Eine Ausnahme ist freilich Thomas Fossen, der im Rahmen seiner Analyse von Habermas' Methode der rationalen Rekonstruktion die Anwesenheit eines »imaginative judgment […] on the part of the theorist« (Fossen 2015: 1080) ausmacht. Da hinter diesem *judgment* unschwer erkennbar die reflektierende Urteilskraft steht, läuft Fossens Argumentation letztlich auf die interessante These hinaus, dass Habermas selbst Anwender einer dezidiert methodisch ausgerichteten reflektierenden Urteilskraft ist.

17 Mit Blick auf das Konzept der *pouvoir constituante* hat Peter Niesen unter Rückgriff auf Habermas'sche Motive jüngst ganz ähnlich (re-)konstruktivistisch argumentiert und betont, dass »through processes of bootstrapping, constitutionalisation within and beyond states typically *produces* its constituent subjects« (Niesen 2019: 38, meine Hervorhebung, TE). Dass Subjekte demnach allererst »*post hoc*« (ebd.) gleichsam durch ihren Gegenstand (»constitutionalisation«) hervorgebracht werden, ist folglich eine Annahme, die im Diskurs der Volkssouveränität durchaus etabliert ist.

18 Eine kluge und zugleich rechtstheoretisch informierte Ausnahme bildet freilich Leora Bilsky (vgl. Bilsky 2008, 2009). Das Motiv der Maske ist aber nicht zuletzt auch deshalb interessant, weil es in Arendts Werk immer wieder vorkommt: So spricht Arendt auch in *Vita activa* beispielsweise von der »Maske des Nutzens« (Arendt 2002: 201) und von »Charaktertypen«, »hinter denen […] das eigentlich Personale sich mit einer solchen Entschiedenheit verbirgt, dass man versucht ist, die Charaktere für Masken zu halten, die wir annehmen, um das Risiko des Aufschlusses im Miteinander zu verringern« (ebd., 223).

weil es – so jedenfalls meine These – interessante Implikationen für die Frage nach der Optik der Arendt'schen Subjekte hat. Verdeutlicht wird durch dieses Motiv nämlich zunächst einmal, dass die in der Literatur recht beliebte These von dem vermeintlichen Votum Arendts für eine face-to-face-Politik (so z. B. Canovan 1983: 287; ähnlich Brunkhorst 1999: 124) schlichtweg nicht zutrifft: Was auch immer die urteilenden Subjekte sehen mögen, ihre Gesichter sind es jedenfalls nicht. Ganz im Gegenteil: Als Maskenträger, und das heißt bei Arendt natürlich: als mit Rechtspersönlichkeit ausgestattete Akteure bleiben die Subjekte vielmehr völlig intransparent füreinander. Ihre intersubjektive Beziehung lässt sich daher einzig noch durch den Aspekt völliger Äußerlichkeit, ja Fremdheit bestimmen – und diese sich fremd bleibende Äußerlichkeit gilt natürlich erst recht für die Welt der inneren, guten wie schlechten Motive: In ihrer ganzen Opakheit bleiben auch diese derart undurchdringlich, dass sie sich kaum je verlässlich charakterisieren lassen und im Normal- wie auch Extremfall sogar eher als Banalitäten erscheinen dürften – als »Banalität des Bösen« (Arendt 2011b) genauso wie als »Banalität des Guten«. Kurzum: Die Maske steht bei Arendt in letzter Instanz für die Ermächtigung, frei und moralfern, ohne weitere Rechenschaft über die Motivlage die eigenen Interessen verfolgen zu dürfen – und zwar in Prozessen des politischen Handelns und Urteilens letztlich genauso wie in solchen der souveränen Selbstgesetzgebung.

Nachdem der Blick auf die Ebene der Subjekte diese unter rechtlichen Gesichtspunkten als opake Maskenträger erscheinen lässt, so muss im Kontext des nun zu betrachtenden Bereichs des Intersubjektiven ein Sinn ins Zentrum rücken, der nicht nur eine sehr reichhaltige Ideengeschichte für sich beanspruchen kann (vgl. Rosenfeld 2011), sondern auch das eigentliche Fundament von Arendts Theorie des Urteilens bildet. In dieser Theorie stellt der *common sense* sicher, dass es überhaupt ein- und dieselben, das heißt identischen Dinge sind, die wir sehen und beurteilen, und er garantiert somit die gemeinsame Wirklichkeit, die bei Arendt »aus einer Gesamtsumme von Aspekten entsteht, die ein Gegenstand in seiner Identität einer Vielheit von Zuschauern darbietet« (Arendt 2002: 72). Als Garant dieser Identität ist der *common sense* selbst erst einmal gar nicht unmittelbar normativ, sondern vor allem: epistemisch,[19] und entsprechend kann er selbst auch nicht als

19 So auch bereits, zutreffend, die Analyse von Rainer Forst, der sich freilich in Gänze auf die Dimension des Politischen bezieht, die ihrerseits »eine entscheidende […] *epistemische* Dimension [hat]. Der gemeinsame Raum ermöglicht einen Common sense, gemeinsame Meinungen und Urteile,

progressiv oder konservativ charakterisiert werden. Er steht vielmehr für das Reservoir an geteiltem Wissen über die gemeinsame Welt; einer Welt freilich, deren Historizität sich unmittelbar auch auf diesen »Wirklichkeitssinn« (ebd.: 265) selbst überträgt. Denn nicht nur kann dieser *common sense* im exakten Gleichschritt mit derjenigen Welt verschwinden, auf die er sich vorzüglich bezieht (vgl. ebd.: 355 ff.), sondern er sollte in weitgehender Entsprechung zur ontologischen Struktur und Verortung dieser Welt tatsächlich auch eher *zwischen* den Subjekten angesiedelt werden und gerade nicht bei oder »in« diesen selbst. Dies erklärt wiederum nicht nur Arendts eigene Lokalisierung des *common sense* im Bereich der »Intersubjektivität« (Arendt 2012: 105), sondern untermauert freilich auch die äußerst engen Grenzen individualisierter Verfügbarkeit: Sowohl der *common sense* selbst als auch die von ihm als Realität ausgewiesene Welt können nämlich überhaupt nur in beständiger intersubjektiver Kommunikation, das heißt im iterativen Dialog entstehen; und aus diesem Grund kann es bei Arendt auch gerade nicht bloß darum gehen, dass ein jeder das Gleiche »von einer anderen Position aus sieht und hört« (Arendt 2002: 71), wie Arendt in *Vita activa* selbst bemerkt, sondern über das solchermaßen Gesehene und Gehörte muss auch fortwährend gesprochen, ja letztlich auch geschrieben werden.[20]

## 3. Auf dem Weg zur souveränen Datengenossenschaft?

Vor dem Hintergrund der zuletzt mit Blick auf Arendt entfalteten Überlegungen zu den Ebenen von Objekt, Subjekt und Intersubjektivität stellt sich

eine geteilte Wirklichkeit, die phänomenologisch betrachtet nur durch den Austausch der *doxai* zustande kommt […,] nur als plurale ›gibt‹ es eine wirkliche Welt« (Forst 2007: 235). Auch Remi Peeters hat darauf hingewiesen, dass »the common sense of which Arendt speaks in *Thinking* is conceptualised as a precondition for every experience and for all *knowledge of reality*. As a result, this common sense can be understood as a cognitive faculty.« (Peeters 2009: 346 f., meine Hervorhebung, TE)

20 Obwohl Arendt nicht den geringsten Zweifel an der immensen Bedeutung von Verschriftlichungsprozessen aufkommen lässt (vgl. z. B. Arendt 2002: 204), ist dieser Aspekt in der Sekundärliteratur bisher kaum systematisch bearbeitet worden. Dies ist nicht nur deshalb schade, weil es im Kontext der Digitalisierung bekanntlich vor allem die Schrift ist, deren Bedeutung sich rapide wandelt – ein Gesichtspunkt übrigens, der womöglich auch das enorme theologische Interesse an der Digitalisierung zu erklären vermag (vgl. Stoellger 2021) –, sondern weil inzwischen auch ein interessanter Diskurs zur Rolle von Schrift, Verschriftlichung und Schreibenden entstanden ist. Vgl. dazu z. B. Amlinger 2021, Sommer 2020.

– nun bezogen auf digitalpolitische Problemstellungen – die Frage, ob und wie sich die damit verbundenen Gesichtspunkte produktiv auf den Diskurs zur Datensouveränität übertragen lassen. Diese Frage nach der Übertragbarkeit möchte ich umstandslos bejahen – und auf mehrere Möglichkeiten verweisen, die wiederum den drei Ebenen des Objekts, der Subjekte und der Intersubjektivität entsprechen. Zunächst lässt sich vor der Folie des oben erläuterten Objekt-Subjekt-Verhältnisses der von Hummel u. a. favorisierten Umstellung von der Input- auf die Output-Orientierung bei der Einwilligung zur Ermöglichung von Datensouveränität unter Bedingungen von Big Data (vgl. Hummel u. a. 2021a: 23) ein anderer Sinn geben: Bestand die obige Pointe nämlich in der nachgelagerten Emergenz der Subjekte im Verhältnis zu den bzw. ihren Objekten, so muss sich auch die Dimension des Outputs nicht mehr nur allein auf die ex ante kaum mehr vorhersehbaren Nutzungskontexte von Daten beziehen, sondern insbesondere auch auf die durch die Daten selbst möglicherweise allererst hervorgebrachten Subjekte. Auf diese Weise kann zugleich die mit der Datennutzung verbundene, teilweise bis ins Extrem gesteigerte epistemische Unsicherheit fairer gestreut werden: Das im Kontext von Big Data niemals sichere Wissen darüber, in welchen völlig neuen Kombinationen eigene Daten auftauchen könnten (vgl. dazu Deutscher Ethikrat 2018: 130 ff.; Nickel 2019), wäre gleichsam flankiert durch eine komplementäre Unsicherheit auf Seiten der großen Datensammler hinsichtlich der Frage, wer sich – aktiviert durch die Masse an Daten selbst – früher oder später als (Kollektiv-)Subjekt konstituieren, an den Verhandlungstisch kommen und wie auch immer machtbasierte Ansprüche geltend machen könnte. Dass es sich dabei derzeit noch um eine rein theoretische und eher optimistische Option handelt, ist natürlich klar; doch gänzlich naiv ist dies nicht: Aus gutem Grund hat der Entwurf des Data Governance Act (DGA) neben den Neuen Intermediären auch die Idee der Datengenossenschaften aufgegriffen (Europäische Kommission 2020b: 20 f., 35) und damit, so ist jedenfalls trotz aller berechtigten Kritik am DGA (vgl. Lanier 2021) zu hoffen, den rechtlichen Startschuss für die auch empirische Entstehung von Kollektivakteuren gegeben, die auf dem hochgradig vermachteten Feld von Daten und Digitalisierung ihrerseits womöglich einiges in die Waagschale werfen könnten. Gleichzeitig wäre mit dieser Herangehensweise im Übrigen auch eine gewisse Entlastungsfunktion für die Theoretikerin eingebaut: Statt nämlich auf dem theoretischen Reißbrett ex ante Akteure entwerfen zu müssen, die als Träger von Datensouveränität

infrage kommen könnten,[21] kann vielmehr ein entspanntes Verhältnis zur Empirie eingenommen und – wie gesagt: mit reichlich kontrafaktischem Optimismus – darauf gebaut werden, dass früher oder später schon diejenigen handlungsfähigen Akteure emergieren werden, die ein legitimes Interesse an ihren Daten haben. Zusätzlich zu den neuen, potenziell kollektiven Subjekten der Datensouveränität lohnt der Blick auf die zweite Ebene, die sich oben mit dem Arendt'schen Motiv der Maske verband. Das Motiv impliziert in erster Linie eine Interessennähe und Moralferne. In diesem Sinne weist es darauf hin, dass die sich leicht einstellenden Gefühle von digitaler Emanzipation, datenbezogener Autonomie und sozialer Fortschrittlichkeit – die zwar allesamt überaus berechtigte Motive artikulieren, aber eben auch schnell romantisierend klingen – wenn nicht durch das Bild eines kühlen Rationalismus ersetzt, so durch dieses doch zumindest ausbalanciert werden sollten. Insbesondere mit Blick auf den in Deutschland bisher kaum beachteten Diskurs um die Datensouveränität von Indigenous Communities (vgl. z. B. Kukutai/Taylor 2016) wird es neben den diversen normativen Vorstellungen in erster Linie darum gehen müssen, diese prozedural zu Artikulation und Durchsetzung ihrer eigenen Interessen zu ermächtigen – zu einer Interessendurchsetzung mithin, die sich im Konfliktfall auch gegen die Interessen der Mehrheit richten können muss. Selbstredend gilt dies auch für die bereits angesprochenen Datengenossenschaften, die ebenfalls nicht mit einem wohlig-warmen Kommunitarismus assoziiert, sondern vielmehr als kühl-rationale kollektive Interessenvertretungen und im Extremfall gar als Kampforganisationen verstanden werden sollten, die sich strukturell auch der Rolle von Gewerkschaften annähern könnten. Da Daten selbst jedenfalls nicht nur einen inhärenten Bestandteil des surveillance capitalism (Zuboff 2019) bilden, sondern längst Kapital sind, liegt es nahe, auch die auf die Daten bezogene Souveränität grob am Vorbild derjenigen klassischen kollektiven Organisations- und Verhandlungsmodi zu orientieren, die schon seit jeher auf den Ausgleich zwischen Kapital und Arbeit gerichtet sind (vgl. Staab/Piétron 2021: 201 ff.), wobei diese dann freilich auch ganz problemlos zur Vorstellung multipler demoi

---

21 Einen guten Überblick über derartige Entwürfe liefert die Literaturschau zur Datensouveränität von Hummel u. a. 2021b. Als Träger von Datensouveränität tauchen dort auf: countries, Indigenous population, user/consumer, private-sector organizations, governmental organizations, non-governmental organizations, expert/professional, societies, citizen, intergovernmental organizations, patient (vgl. ebd.: 4).

sektoraler Art (siehe schon Abromeit 1999) oder auch funktionaler Ausrichtung erweitert werden könnten bzw. sollten. Am Ende des Tages könnte die Datengenossenschaften jedenfalls nichts und niemand daran hindern, die Semantik der Demokratie für sich zu beanspruchen oder sich gar als demokratische demoi zu konstituieren – demoi welchen Zuschnitts auch immer.

Dass jedenfalls eine starke Präsumtion nicht nur zugunsten kollektiver, sondern vor allem auch institutionalisierter Organisationsformen besteht, ist eine Konsequenz, die sich schließlich auch vor dem Hintergrund der an Arendt geschärften Überlegungen zum im Bereich des Intersubjektiven angesiedelten common sense ergibt. Es wurde bereits darauf hingewiesen, dass dieser dezidiert zwischen den Subjekten angesiedelte Sinn im fortlaufenden, stabilen Dialog zugleich Wirklichkeitswissen produziert. Für die Datensouveränität folgt daraus zunächst, dass das mit der Datensouveränität verbundene Konzept des *dynamic consent* (vgl. Hummel u. a. 2021a: 13–20, zuvor schon Hummel u. a. 2018) offenkundig nicht derart »dynamisch« sein darf, dass es letztlich doch nur einsame, atomisierte Individuen sein können, die ihre Präferenzen, etwa im Rahmen automatisierter Einwilligungsprozesse, gänzlich dialogfrei anpassen (lassen) und dabei allerhöchstens noch mit Algorithmen kommunizieren; in der Arendt'schen Theoriesprache wären sie damit letztlich welt- und wirklichkeitslos. Intersubjektive Kommunikation über den Sinn von Datenweggabe und Datennutzung müsste vielmehr auch im Lichte des *dynamic consent* in stabile, und das heißt gerade: nicht-dynamische Formate eingebunden werden, deren Stabilität nicht nur ein Mindestmaß an Institutionalisierung verlangt, sondern auch den wie auch immer beiläufigen Austausch von Wissen ermöglichen muss. Neben der Notwendigkeit der stabilen Institutionalisierung setzt just dieser Aspekt intersubjektiv geteilten, insofern kollektiven Wissens indes auch dem unvermittelten Zugriff auf kontroverse normative Konzepte durchaus Grenzen – dies zumindest dann, wenn dieser Zugriff gewissermaßen monologisch, aus den Hinterzimmern politischer oder juristischer Experten heraus erfolgt, die ein überlegenes Wissen auch in normativen Fragen beanspruchen. Vor diesem Hintergrund stellt sich dann nicht zuletzt auch die Frage, ob es denn überhaupt sachdienlich ist, die mit Datensouveränität konnotierten Subjekte nicht so sehr mit Demokratie und Volkssouveränität, dafür jedoch umso stärker mit allerlei materiell hochgradig aufgeladenen normativen Begriffen wie Gerechtigkeit

und Solidarität (vgl. Deutscher Ethikrat 2018: 219–225, 226–229)[22] oder auch Gemeinwohl und Würde (vgl. Staab/Piétron 2021) zu assoziieren. So wichtig und richtig diese normativen Konzepte auch zweifellos sein mögen, am Ende des Tages formulieren sie nicht nur eine sehr anspruchsvolle normative Messlatte, an der die schnöde interesseninfiltrierte Realität datensouveräner Akteure und also auch der Datengenossenschaften vermutlich nur wird scheitern können; zudem mag sich schlussendlich auch herausstellen, dass einzig eine wohldosierte und dezidiert demokratische Normativität es überhaupt noch vermag, orientierende Schneisen in das kaum noch zu entwirrende Dickicht aus Recht und Ethik[23] zu schlagen, das die »Digitale Konstellation« (Berg/Rakowski/Thiel 2020; vgl. Hofmann 2019) inzwischen umgibt. Eine demokratietheoretisch ausbuchstabierte und mit dem Prinzip der Volkssouveränität verbundene Idee der Datengenossenschaft könnte beim Schlagen genau dieser Schneisen womöglich behilflich sein.

22 Vgl. allerdings zu dem Versuch, einen nicht so sehr normativ-moralischen, sondern eher objektivistischen Begriff von Solidarität zu entwickeln, die auf die soziologische bzw. französische Ideengeschichte rekurrierenden Arbeiten von Hermann-Josef Große Kracht, z. B. Große Kracht 2017.

23 Vgl. zu diesem »Dickicht« den zutreffenden Hinweis von Florian Möslein auf die Verrechtlichung der Ethik und die umgekehrte »Ethisierung des Rechts« (Möslein 2020: 41). Überhaupt scheint das Bild der Entgrenzung der bestimmende Topos der Digitalen Konstellation zu sein. Dieser betrifft beispielsweise auch das Verhältnis zwischen Privatheit und Öffentlichkeit im Kontext der Sozialen Medien, vgl. dazu Staab/Thiel 2021.

# Datensouveränität als Gestaltungskonzept wissenschaftlich-technischer Entwicklungen

*Stefan Gammel und Jan Cornelius Schmidt*

## 1. Einleitung

Neue Begriffe sind zentraler Teil gesellschaftlicher wie wissenschaftsinterner Aushandlungsprozesse. Kaum ein Begriff ist in der bundesdeutschen Digitalpolitik derzeit so schillernd und schnörkelhaft, so prominent und programmatisch wie der der Datensouveränität. Gleichzeitig erscheint der Begriff weithin komplex, plural, undurchsichtig – und er ist, recht besehen, umstritten. So liegt als Diagnose nahe, dass es sich bei Datensouveränität um einen Begriff handelt, dessen Verwendungsweise ein »considerable degree of divergence and an occasional lack of clarity about intended meanings« zeigt (Hummel u. a. 2021b: 1; vgl. auch Couture/Toupin 2019).

Im Folgenden wird dargelegt, dass der Begriff keineswegs derart unbestimmt ist, sondern in zwei Hauptverwendungsweisen auftritt. Die beiden Verwendungsweisen können mit der philosophischen Tradition, etwa mit der Freiheitsthematik, in Verbindung gebracht werden. Gerade die zweite Verwendungsweise, die insbesondere im deutschsprachigen Diskurs eine große Verbreitung aufweist, signalisiert politische wie individuelle Gestaltungsherausforderungen, die ein hybrides Feld von Wissenschaft, Technik, Wirtschaft, Politik und Lebenswelt umfassen. Notwendig erscheinen Klärungsanstrengungen, um die mit dem Begriff verbundene Gestaltungsoptionen avancierter wissenschaftlich-technologischer Entwicklungen zu erarbeiten und in Anschlag zu bringen. Dabei gilt es, eine Perspektive zu verfolgen, aus welcher nicht nur der individuelle Endnutzer, Konsument und Bürger zur Verantwortung gedrängt wird. Vielmehr müssen unterschiedliche Akteursebenen zusammenspielen. Es wird für ein flexibles, adaptives, kontextsensitives Gestaltungsmodell argumentiert, welches eine

Nähe zur lebensweltlichen Verwendungsweise des Souveränitätsbegriffs im deutschen Sprachraum aufweist.

## 2. Anlässe

In der letzten Dekade ist der Begriff der Datensouveränität ins Zentrum der Digitalpolitik gerückt, insbesondere im deutschen Sprachraum.[1] Es kann von einem politischen Trendbegriff gesprochen werden. Das sollte nicht darüber hinwegtäuschen, dass – genau besehen – der Begriff deutliche Spannungen und Konfliktpotenziale in sich trägt. Zur breiten Popularität tragen zwei unterschiedliche Anlässe bei.

Ein erster, eher traditioneller Anlass für die Begriffskarriere von Datensouveränität liegt in der Diagnose einer Bedrohung oder eines Verlusts an staatlicher oder verbundstaatlicher Handlungs-, Kontroll- und Durchsetzungsfähigkeit, verbunden mit reduzierter nationaler oder EU-transnationaler Innovations- und Wettbewerbsfähigkeit. Dieses als traditionell anzusehende Verständnis von (Daten-) Souveränität ist territorial und national bzw. transnational ausgerichtet, es bezieht sich etwa auf Deutschland oder die EU in räumlicher Hinsicht. So wird etwa in einem Entschließungsantrag im Bundesrat unter dem Titel »Europäische Datensouveränität schützen« herausgestellt, dass der

> »Debatte um eine technologische Souveränität […] auch eine intensive Diskussion um eine europäische Datensouveränität folgen muss […]. Dies ist nur dann zu gewährleisten, wenn der Gesetzgeber einen festen Rahmen, insbesondere im Hinblick auf Datenschutz und Wettbewerb setzt. […] Nur so können europäische Werte, wie das Recht auf informationelle Selbstbestimmung, einen wirksamen Schutzraum darstellen.« (Bundesrat 2021)[2]

In diesem Sinne scheint die Souveränität der EU durch Russland oder China bedroht, insofern befürchtet wird, dass diese Staaten in europäische (staatliche oder Unternehmens-) Rechnersysteme eindringen, Wahlprozeduren verfälschen, Unternehmensdaten ausspionieren oder (kritische) Infrastrukturen angreifen. Mitunter wird – in abgeschwächter Form – auch

1 Siehe den Beitrag von Gehring in diesem Band.

2 Der ehemalige Außenminister Fischer stellte ähnlich heraus: »Europa wird also als wichtigste Aufgabe seine Datensouveränität sichern müssen. Das wird sehr große materielle Ressourcen und eine entschlossene Aufholjagd gegenüber den USA und China erfordern, denn im Augenblick droht Europa, weil viel zu langsam und unentschlossen, abgehängt zu werden.« (Fischer 2019).

eine Souveränitätsbedrohung durch starke Abhängigkeiten der deutschen Bundesverwaltung von bestimmten Software-Anbietern gesehen, z. B. von Microsoft-Produkten.[3]

Weitere Beispiele dieser Position finden sich im europäischen Umfeld sowie im internationalen Diskurs (vgl. Hummel u. a. 2021b): »[M]any governments have raised concerns about national data sovereignty when government information is moved to the cloud.« (Irion 2012: 41) Oder auch: »Data sovereignty is the concept that information, which has been converted and stored in binary digital form, is subject to the laws of the country in which it is located« (Hippelainen u. a. 2017: 645). So entsteht die Notwendigkeit eines neuen, international kompetitiven Politikfeldes, was in Deutschland oftmals als Digitalpolitik bezeichnet wird:

> »At the national level, the capacity of accumulating, processing, and utilizing vast amounts of data will become a new landmark of a country's strength. The data sovereignty of a country in cyberspace will be another great power-game space besides land, sea, air, and outer spaces« (Jin u. a. 2015).[4]

Auch wenn zwischen englisch- und deutschsprachigen Wortbedeutungen, das heißt zwischen »Data Sovereignty« und »Datensouveränität« gewiss zu unterscheiden ist, finden sich im deutschen Sprachraum entsprechende Verwendungsweisen, die eine semantische Nähe oder gar Äquivalenz nahelegen.[5] So kann man sagen, dass Teile dieses internationalen Diskurses

---

3 Zu diesem Ergebnis kommt eine vom Innenministerium in Auftrag gegebene Studie (PwC 2019).

4 Ähnliche Hinweise und Diskussionslinien finden sich in anderen Papieren: »From Indonesian policy makers' perspective, the term ›data sovereignty‹ is not yet in use, but it refers to the national legislation on the state defence against external threats such as state-actors and non-state actors« (Nugraha u. a. 2015; nach: Hummel u. a. 2021b: 7). Vielleicht noch deutlicher: »One could even assert that national sovereignty is conditional upon adequate data sovereignty. If a country has no effective means of controlling public information it will become in parts dysfunctional« (Irion 2012: 53). »Data sovereignty concerns legislation, e.g. when »[t]he concept of ›data sovereignty‹ […] refers to both specific data sovereignty laws limiting cross-border data transfer, as well as the more general difficulty of complying with foreign legal requirements« (Vaile 2014). Somit gilt zusammenfassend: »Data sovereignty can apply to a range of agents across the spectrum from individual consumers to entire societies and countries, sometimes yielding conflicting claims to data sovereignty across these levels." (Hummel u. a. 2021b: 15) Ähnlich äußern sich Rainie u. a. (2017: 5 f.): »[D]ata sovereignty is the right of a nation to collect and manage its own data« – allerdings im spezifischen Kontext des Strebens indigener Bevölkerung, das Sammeln ihrer Daten durch andere Nationen im kolonialistischen Zusammenhang zu verhindern. Souveränität gegenüber Firmen wie den GAFA sind hier kein Thema.

5 Einige Belege wurden oben angegeben. Weitere sind: »Gaia-X ist eine vernetzte Dateninfrastruktur […] auf europäischer Ebene. Der Bundesrepublik müsse es gelingen, die eigene Datensouve-

in Deutschland dem Begriff nach aufgenommen wurden. Allgemein gibt es hier auch Überschneidungen zum Begriffsfeld der digitalen Souveränität.[6]

Unter »Datensouveränität« wird in dieser Verständnisweise und Argumentationslinie primär eine territoriale Abwehr von äußeren Einflüssen, wie etwa anderer Länder, multinationaler Konzerne oder Plattformbetreibern, und eine Wiederherstellung von nationalen oder transnationalen Entscheidungs- und Kontrolloptionen gefordert. Der Diskurs um Datensouveränität als Abwehrkonzept umfasst damit Machtfragen und machtpolitische Dimensionen, auch solche, die eine globale Weltwirtschaft oder, wie von Kritikern akzentuiert, einen digitalen Kapitalismus in den Blick nehmen. Transnationale Regulationsoptionen werden anvisiert; ob und wie welche Regulationen praktikabel sind, wird kontrovers diskutiert.

Als zweiter, zu unterscheidender Anlass kann die Wahrnehmung und Diagnose angesehen werden, dass der herkömmliche Datenschutz in unterschiedlichen Hinsichten defizitär ist – er sei neu zu denken und anders zu implementieren. So sieht die »Initiative D21« die Einführung des Begriffs Datensouveränität als Versuch an, mit dem »Dilemma des Datenschutzes« umzugehen und Auswege zu sondieren (Horn/Stecher 2019: 1). Denn einerseits werde »die Praxis« dem »eigentlichen Ziel des Datenschutzes« angesichts der global-transterritorialen technologisch-ökonomischen Entwicklung »nicht gerecht« (ebd.: 2): Traditioneller Datenschutz könne die Daten von Personen, Unternehmen, Institutionen und Staaten nicht hinreichend schützen. Andererseits behindern zu restriktive und unflexible Regulierungen, die dem herkömmlichen Datenschutzkonzept inhärent seien, technologische, ökonomische und soziale Innovationen – und vielfach auch weitergehende Partizipationsmodalitäten von Bürgern und Konsumenten.

ränität zu gewährleisten und dazu gehöre eine eigene Dateninfrastruktur […] Gaia-X ist schon als Alternative zu amerikanischen und chinesischen Anbietern gedacht.« (Bundesregierung o. J. [2020]); »Schon seit einiger Zeit fordern Datenschützer und Netzexperten, dass Deutschland für ›Datensouveränität‹ sorgen soll, um sensible Daten der Bürger […] gefahrlos verarbeiten und speichern zu können. Geplant ist deshalb eine eigene Cloud, in der die Daten gespeichert werden können, ohne dass amerikanische Behörden Zugriff haben« (Budras 2021); oder auch: »Im politischen Diskurs wird der Begriff der Datensouveränität verwendet, um den angestrebten Zustand der Unabhängigkeit von ausländischen Datenverarbeitungsunternehmen zu bezeichnen« (Smart Data Forum o. J.).

6 Das Bayerische Forschungsinstitut für Digitale Transformation, welches institutionell der Bayerischen Akademie der Wissenschaften zugeordnet ist, führt aus: »Sehr weit verbreitet ist aber auch ein überindividuelles Verständnis des Konzepts ›Datensouveränität‹, das dann als gleichbedeutend mit ›digitaler Souveränität‹ aufzufassen ist.« (bidt o. J. [2022]).

So erscheint der Diskurs um Datensouveränität als ein Grundlagendiskurs über Datenschutz, der nach Ziel und Praxis, nach Fehlentwicklungen und Fortentwicklungsoptionen des Datenschutzes (in Deutschland und in der EU) fragt.

Eine ähnliche Anlassbeschreibung findet sich beim Deutschen Ethikrat. So sei das »Datenschutzrecht […] auf das Phänomen Big Data unzureichend eingestellt«[7] und »zentrale Prinzipien und Zielvorgaben des überkommenen Datenschutzrechts« seien »mit den Besonderheiten von Big-Data-Anwendungen kaum in Einklang zu bringen«, um ein »hohes Datenschutzniveau« zu sichern (Deutscher Ethikrat 2018: 128 f.). Auf der anderen Seite könnten etwaige Chancen und positive Perspektiven der technologischen Entwicklung von KI, Big Data und Machine Learning im Rahmen der herkömmlichen Datenschutzregulationen (Personenbezug, Zweckbindung, Datensparsamkeit, Transparenz, datenspezifische Einwilligungserfordernis) nicht hinreichend genutzt werden. Mit anderen Worten: »Will man weder den Einsatz von Big Data grundsätzlich untersagen [und soziotechnologische Innovationen verhindern] noch relevante Einbußen am [Daten-] Schutzniveau hinnehmen, müssen alternative Gestaltungsoptionen und Regelungsmechanismen entwickelt werden.« (ebd.: 130) »[F]lexible, innovationsoffene Regelungen« müssen gefunden werden. Noch deutlicher in Richtung Innovationsverstärkung führte der damalige Wirtschaftsminister Sigmar Gabriel zur Eröffnung des neunten Nationalen IT-Gipfels aus:

> »Der traditionelle Datenschutzbegriff, den wir haben, ist für das Thema digitale oder datengestützte Ökonomie nicht mehr wirksam. Der Auftrag unserer Datenschutzgesetze, Daten sozusagen zu minimieren, ist sozusagen das Gegenteil dessen, was wir für die Wettbewerbsfähigkeit in einem digitalen Zeitalter brauchen. Stattdessen geht es um Datensouveränität« (Gabriel 2015; vgl. auch: Krempl 2015; Hummel u. a. 2021b: 7).

Ob *beides* gleichzeitig – effektiver Datenschutz *und* weitreichende soziotechnologische Innovationen – möglich ist, wie von vielen Befürwortern des Begriffs Datensouveränität angenommen, etwa von der Initiative D21 und dem Deutschen Ethikrat, ist offen. Dies hängt nicht nur vom technologischen Stand und Informatik-inhärenter technisch-algorithmischer Optionen sowie etwaiger Regulierungsoptionen ab, sondern entscheidend

7 Zu KI und Big Data siehe: Schmidt 2022 und allgemein Gethmann u. a. 2022.

ist, was unter effektivem Datenschutz und unter Innovationen verstanden werden soll.

Damit gibt es zwei Anlässe der Begriffskarriere von Datensouveränität: erstens, die Suche nach (neuen) nationalen oder transnationalen Abwehrmechanismen gegenüber möglichen Eingriffen, Abhängigkeiten und Kontrolloptionen durch andere Staaten, Konzerne oder Personen – verbunden mit dem Ziel der Sicherstellung nationaler oder transnationaler (z. B. EU-) Souveränität; zweitens, die Suche nach einem qualitativ anderen und neuen Datenschutzkonzept unter einem neuen Begriff, so dass Defizite beseitigt werden und insbesondere Innovationen ermöglicht werden. Der erste Anlass weist Überschneidungen mit dem Begriffsfeld der »digitalen Souveränität« auf, der zweite Anlass kann als spezifisch für den deutschen Diskurs angesehen werden. Er gewinnt zunehmend an Bedeutung und versucht, über einen abwehrorientierten Risikodiskurs Gestaltungsoptionen in den Blick zu nehmen, was indes nicht nur als ambitioniert, sondern auch als ambivalent anzusehen ist.

## 3. Eine eher traditionelle Sichtweise auf Risikoaspekte – Datensouveränität als Abwehr- und als Schutz-Konzept und als negative Freiheit

In den zwei Anlässen spiegeln sich, so unsere Diagnose, vier Diskurslinien um Datensouveränität wider, in deren Rahmen unterschiedliche, teils konfligierende, teils ergänzende Hintergrundüberzeugungen identifiziert werden können.

Zunächst gibt es staatliche, politische und ökonomische Abwehrmotive (1) (erster Anlass, siehe oben). Diese richten sich auf die Sicherung von nationaler oder EU-Souveränität (i. A. verstanden als vom Volk dem demokratisch legitimierten Parlament, der Regierung und weiteren staatlichen Institutionen verliehene nationale Entscheidungs- und Durchsetzungsgewalt) durch territoriale Abwehr von äußeren Einflüssen, wie jenen von Konzernen und Plattformbetreibern, von Drittstaaten oder Kriminellen. – Verwandt zu diesen Motiven sind sodann die eines effektiven (rechtlich garantierten und/oder technisch via Design implementierbaren) Datenschutzes (2), der ebenfalls auf eine Abwehr des Zugriffs und der Einflussnahme auf personenbezogene oder Unternehmens-Daten durch Plattform-

und Digitalindustrie, durch Kriminelle oder auch durch den Staat – und somit auf eine Sicherstellung von *Privacy* und informationeller Selbstbestimmung – zielt (Teile des zweiten Anlasses). Es geht dem Datenschutzmotiv um Herstellung und um Durchsetzung adäquater Rahmenbedingungen für selbstbestimmtes individuelles, institutionelles oder unternehmerisches Handeln im digitalen Raum. – Allgemein sind die Abwehrmotive (ad 1) territorial nach *außen* gerichtet, während die Datenschutzmotive (ad 2) sich insbesondere nach *innen* orientieren, freilich aber auch auf eine Abwehr von äußeren sowie von inneren Einflüssen unterschiedlicher Akteursgruppen zielen.

Diese beiden Motivtypen können, analog zu negativen Freiheitsbegriffen, als negative Konzepte von Datensouveränität verstanden werden. Es geht jeweils um Sicherung, Aufrechterhaltung oder Herstellung von Handlungsgewalt, verstanden als (Daten-) Souveränität *von* bzw. *gegenüber* Zu- und Eingriffen von Dritten, also um Abwehr und Schutz der Souveränität *gegen(-über)* andere(n), analog zu (negativer) Freiheit als Freisein *von* Zwängen (z. B. Leibniz).[8] Historisch weisen diese Konzepte eine Nähe zu staatsrechtlichen Souveränitätsverständnissen auf – ein traditionsreicher Diskurs der politischen Philosophie, der mit der Begriffsprägung durch den französischen Parlamentsjuristen und politischen Theoretiker Jean Bodin (1529–1596) begann.

Wenn in der aktuellen Debatte unter Datensouveränität eine Sicherung von nationaler Handlungs-, das heißt Entscheidungs- und Durchsetzungsmacht im Sinne territorialer Abwehr von äußeren Einflüssen angemahnt wird (ad 1), dann schwingt der staatsrechtliche und -philosophisch-historische Diskurs um äußere oder nationale Souveränität des Territorialstaates mit. Diese wurde darin gesehen, dass der Staat, insofern er Souveränität besitzt bzw. diese vom Volk temporär verliehen bekommt, als solcher über Handlungsgewalt verfügt, das heißt dass er unabhängig von Befehlen und

8 Eine ähnliche Unterscheidung von Freiheit – als positive bzw. negative Freiheit – findet sich bei Isaiah Berlin (1969: 121 f), wobei der Text 1958 verfasst ist. »The first of these political senses of freedom or liberty (I shall use both words to mean the same), which (following much precedent) I shall call the ›negative‹ sense, is involved in the answer to the question ›What is the area within which the subject – a person or group of persons – is or should be left to do or be what he is able to do or be, without interference by other persons?‹ The second, which I shall call the ›positive‹ sense, is involved in the answer to the question ›What, or who, is the source of control or interference that can determine someone to do, or be, this rather than that?‹ The two questions are clearly different, even though the answers to them may overlap.«

Einflüssen anderer ist, etwa vom Papst, von einem Kaiser oder allgemein von einem Herrscher eines anderen Staates. Historisch konnte sich die Handlungsgewalt auch darauf beziehen, nicht in einem Tributs-, Vasallen- oder ähnlichem Abhängigkeitsverhältnis zu stehen.[9]

Semantisch ähnlich, im Detail – was die »Stoßrichtung« der Abwehr-Aktivität angeht – anders ausgerichtet als die oben genannte äußere Souveränität richtet sich der Souveränitätsdiskurs um Datenschutz (auch) nach innen (ad 2).[10] Zunächst kann man in Anlehnung an den staatsrechtlichen Diskurs der europäischen Kulturgeschichte sagen, dass der Staat als Souverän innere Souveränität besitzt, für seine Bürger und die auf seinem Rechtsterritorium Handelnden Gesetze zu erlassen und durchzusetzen – und zwar unabhängig von einzelnen partikulären Interessensgruppen. Wer hingegen zur Rechtsdurchsetzung auf die Unterstützung anderer Instanzen angewiesen ist,[11] ist im Bodinschen Sinne nicht souverän. Innere Souveränität wird heute herausgefordert von Interessengruppen der internationalen Digitalindustrie, insofern diese in Deutschland territorial agieren, viele deutsche Nutzer haben und deutschsprachige Foren bedienen. Dass zumindest partiell innere Souveränität gegeben ist, zeigt sich in der rechtlichen Verpflichtung beispielsweise Facebook gegenüber, auf ihren Webseiten Hass und Hetze zu identifizieren und zu eliminieren, was partiell auch realisiert wird. Grenzen der inneren Souveränität werden sichtbar im Falle von Cambridge Analytica oder auch vom Messengerdienst Telegram, wo die Rechtsdurchsetzung der Schutzmotive misslingt. Wesentlicher Akteur, dem Souveränität in diesem Sinne zu- oder abhandenkommt, ist der Staat: Schutz nach »außen« und »innen«; letzteres meint insbesondere Handlungsgewalt und Rechtsdurchsetzung nach »innen«.

Allerdings muss man sagen, dass der Souveränitätsdiskurs um Datenschutz über die oben genannte innere Souveränität und dem damit verbundenen Focus auf den Akteur Staat, das heißt über Fragen nach der Souveränität des Staates und nach dem Staat als Souverän, hinaus geht. Schließlich steht angesichts der globalen Digitalisierung die Handlungsgewalt und Selbstbestimmung (»Autonomie«, »Mündigkeit«) von

9 Siehe auch den Beitrag von Gehring in diesem Band. Zu betonen ist, wie Bodin bereits ausführt, dass Souveränität nicht unbeschränkt ist, sondern durchaus an eine vorgegebene Ordnung gebunden ist bzw. sein kann (Grimm 2009; Brunhöber 2011).

10 Wenngleich eine Abwehr gegenüber äußeren Einflüssen eine allgemein notwendige Bedingung zur Ermöglichung von Datenschutz darstellt.

11 Traditionell etwa Stände, Klerus, Adel oder Stadtbürger.

Individuen, Institutionen und Unternehmen in Frage – mit anderen Worten: die individuelle, institutionelle bzw. unternehmerische Souveränität wird fragwürdig.[12] Um die Möglichkeit der Souveränität dieser Akteure zu sichern, ist der Datenschutz (durch den Akteur Staat) zu stärken: Nur ein verbesserter Datenschutz könne demnach, so kann man diese Position zusammenfassen, die Bedingung der Möglichkeit *gegen* Einflussnahme Dritter schaffen, wobei der Staat die rechtlichen Rahmenbedingungen bereitstellt. Die Souveränität des Staates könne durch starke Datenschutzregulierung die Sicherung oder gar partielle Weitergabe der Souveränität an Bürger, Institutionen und Unternehmen ermöglichen – als Kompetenz des Staates, Kompetenz weiterzuleiten, kurz: als Kompetenz-Kompetenz. Gleichzeitig sei diese Ermöglichung und Weitergabe als solche ein Zeichen, Souveränität zu haben. Souverän ist derjenige, der Souveränität anderen ermöglicht: Der Staat ist souverän, insofern er seinen Bürgern Räume eröffnen kann, in denen sie souverän (u. a. privatautonom) handeln können.

Zusammengenommen findet sich in den Abwehr- und Schutz-Diskursen eine doppelte Referenz: Einerseits ist die Durchsetzung von Abwehr- und Schutzmaßnahmen selbst ein zentrales Zeichen oder wesentliches Charakteristikum von (äußerer und innerer) Souveränität. Wenn ein Akteur (hier: beispielsweise der Staat) die Abwehr- und Schutzmaßnahmen realisieren kann, dann *ist* er souverän bzw. *hat* er Souveränität. Andererseits sind Abwehr- und Schutzmaßnahmen als Bedingung der Möglichkeit von Souveränität anzusehen – als Ermöglichungsbedingungen. So sichert oder ermöglicht die Abwehr (z. B. durch die EU-Staatengemeinschaft) nach außen gegenüber Eingriffen dem Staat (nationale bzw. innere) (Daten-) Souveränität. Und die Durchsetzung von staatlichen Schutzmaßnahmen (z. B. Datenschutzrecht) ermöglicht individuelle, institutionelle oder unternehmerische Souveränität im Inneren. Aus letzterer Perspektive ist Datenschutz nicht durch Souveränität ersetzbar, weil der Datenschutz eine zentrale Ermöglichungsbedingung von Souveränität darstellt. Nimmt man die doppelte Referenz zusammen, kann eine Abfolge von Ermöglichungsbedingungen angegeben werden, die jeweils notwendige, aber keine hinreichenden Bedingungen darstellen: Die äußere (staatliche) (Daten-) Souveränität kann als Bedingung von innerer (staatlicher) Souveränität angesehen werden, wobei diese ihrerseits erst eine Rahmenbedingung individueller, institutioneller oder unternehmerischer Souveränität darstellt.

---

12 Vorausgesetzt, es hat diese bisher gegeben.

## 4. Datensouveränität als positive Gestaltungsherausforderung – als Freiheit-*zu*

Anders gelagert und konträr zu oben beschriebenen Abwehr- und Datenschutzmotiven sind weitere Motive, nämlich solche, die sich auf Verstärkung und Beschleunigung von Innovationen sowie auf die Nutzung der Chancen eines breiteren Einsatzes von KI, Big Data und Machine Learning beziehen (siehe oben den zweiten Aspekt des zweiten Anlasses) – ein Diskurs, der sich unter dem Label Datensouveränität insbesondere in der bundesdeutschen Digitalpolitik findet. Datensouveränität verspricht modifizierte Regulierungstypen, die anders ansetzen und andere Ziele verfolgen als diejenigen, die derzeit im deutschen oder europäischen Datenschutzrecht realisiert sind. So wird etwa die DSGVO mit ihren Kriterien der Datensparsamkeit und vor allem der *Ex-ante-*Zweckbestimmung als Innovations-hinderlich und allzu risikofixiert angesehen. Daten sollen freier und schneller zirkulieren, sie sollen besser geteilt, genutzt und verwertet werden können als bisher, Datenspenden sollen vereinfacht werden.

Diese Motive sind nun einerseits ökonomisch geprägt (3), sie finden sich bei Unternehmen (insbesondere der Digital- und Plattformindustrie) sowie bei Konsumenten und Endnutzern – und natürlich auch in der Politik. Neben ökonomischen Motiven stehen andererseits solche in Gesellschaft, Politik, Wissenschaft und Kultur (4), die verstärkt die Chancen von KI, Big Data und Machine Learning für die Wissensgesellschaft allgemein ergreifen möchten, wie etwa Forschungs- und Wissenschaftsinstitutionen, Patienten- und Ärztevereinigungen, Rechtsinstitutionen, Strafverfolgungs- und Überwachungsbehörden, u. a. Diese Motive werden auch von jenen zivilgesellschaftlichen Akteuren, Bürgerinnen und Bürgern geteilt, die sich von einer beschleunigten Technisierung und vertieften Digitalisierung breitere gesellschaftliche und politische Partizipationsmöglichkeiten versprechen und damit (basis-) demokratische Prinzipien als erweiter- und ausbaubar ansehen. Auf dieser Linie liegen auch Protagonisten der nachhaltigen Entwicklung und der Nachhaltigkeitstransformation, die aus normativer Perspektive zur Umsetzung der von der UN verabschiedeten Sustainable Development Goals (SDGs) die Megatrends Digitalisierung und Nachhaltigkeit zusammenführen wollen.[13] Vergleichbare Nutzungsinteressen finden

13 Im Aktionsplan des BMBF *Natürlich. Digital. Nachhaltig* heißt es beispielsweise: »Vertrauen und Akzeptanz sind die unabdingbare Voraussetzung für die Nutzung der vielfältigen Chancen der

sich weitergehend bei Widerstandsbewegungen in autoritären Regimen und allgemein bei staatskritischen/-skeptischen oder libertären Gruppierungen.

Auch wenn mit dem Begriff Datensouveränität hier (Punkte 3 und 4) im Detail divergierende Motive verbunden sind, zielen sie alle auf Innovationsermöglichung und -erleichterung sowie auf breitere Nutzungs- und Anwendungspraxen. Hoffnungen, Versprechungen und Visionen einer vertieften und umfassenderen Digitalisierung und Technisierung stehen im Mittelpunkt. So kann man – abermals analog zum Freiheitsdiskurs, hier: zur positiven Freiheit – sagen, dass Innovations- und Nutzungsinteressen positive Visionen von (und durch) Datensouveränität darstellen. Positive Datensouveränität wird nicht vor dem Hintergrund einer weitreichenden Risikowahrnehmung konzipiert, sie ist nicht primär als Abwehr, Schutz und Sicherung, eben nicht als Datensouveränität-*gegen(über)* bzw. *-von* zu verstehen, sondern als Datensouveränität-*zu* oder *-für* (etwas). Was mit dem *Zu* oder *Für* jeweils gemeint ist und qualifiziert wird, kann freilich differieren. Diese Offenheit ist nicht verwunderlich, insbesondere wenn man semantische Überlappungen zur sozialphilosophischen Freiheitsthematik und weitergehend zum weiten Feld des Libertarismus in den Blick nimmt. Datensouveränität wird mit »Freiheit« (explizit oder implizit) in Verbindung gebracht: Datensouveränität *für* eine Ermöglichung und Gestaltung von Freiheit bzw., weitreichender, Datensouveränität *als* (Charakteristikum von) Freiheit. Allgemein stellen Libertäre einen individuellen und/oder wirtschaftlichen Freiheitsgewinn *zur* Entfaltung von Potentialen (z. B. zur Selbstentfaltung, technische Erfindungen, Innovationspotenzial) durch Datensouveränität in Aussicht, einhergehend mit vertieften Möglichkeiten einer individuellen oder wirtschaftlich-unternehmerischen »Freiheitsgestaltung«.[14]

Die meisten Spielarten des Libertarismus verbindet eine staats-, regelungs-, institutionen- und verwaltungskritische Grundhaltung, die dem Staat, wenn überhaupt, nur noch die weithin passive Rolle eines Garanten geeigneter Rahmen- und Randbedingungen zuweist. In der Kritik an klassischen wirtschaftsliberalen Positionen, auch an neueren neoliberalen

---

Digitalisierung für die Gesellschaft und für eine nachhaltige Entwicklung. Dafür müssen Fragen zu Sicherheit, Datenschutz, Datensouveränität und dem Recht auf informationelle Selbstbestimmung adressiert werden.« (BMBF 2020: 12).

14 Eine ähnliche Position vertritt beispielsweise der Deutsche Ethikrat (2018) zur »individuellen Freiheitsgestaltung«.

Sichtweisen, wurde von einer »Nachtwächterrolle« des Staates gesprochen, wie schon von Ferdinand Lassalle (1919) im Jahre 1862 in Reaktion auf Adam Smiths Werk *Wohlstand der Nationen* (1776) und seinem klassischen Konzept des Liberalismus. Eine derart schwache Rolle des Staates wird vermittelnd von ordoliberalen Wirtschaftstheoretikern stets zurückgewiesen: Für sie hat ein starker Rechtsstaat für Individuum und Wirtschaft eine freiheitskonstitutive und -bewahrende Funktion. Am äußersten Rand des Diskurses um Datensouveränität finden sich – analog zum breiten Spektrum des Libertarismus – anarchistische Positionen, die selbst einen Minimalstaat ablehnen, was an frühe Visionen und utopistische Erzählungen des Silicon Valley der 1970er und 1980er Jahren anschließt.

Jenseits von Positionen, die eine libertaristische Sicht verfolgen und dem Begriff oder zumindest der Sache nach einen Rekurs auf Freiheit vornehmen, findet sich in pragmatischeren Zugängen kaum das Pathos von Freiheit. Datensouveränität soll Möglichkeiten erweitern – und in diesem schwachen Sinne neue Freiheiten eröffnen: in und für Forschung und Technologie, Medizin und Strafverfolgung, Demokratie und Nachhaltigkeit, u. a. Aus dieser Sicht ist der Staat nicht zu reduzieren oder gar zu eliminieren, sondern er ist (analog zu vielen Spielarten des Ordoliberalismus) notwendig, um einen adäquaten (Rechts-) Rahmen zur Sicherung und Förderung der beschriebenen gesellschaftlichen und wirtschaftlichen Handlungsfelder zu gewährleisten. Es zeigt sich hier eine Mischung der oben genannten Motivtypen.

## 5. Die Kehrseite: Zuviel (moderner) Technikoptimismus?

Während die Abwehr- und Schutzmotive eher als wohletabliert und weitverbreitet, aber auch als konservativ und risikoorientiert einzuschätzen sind, ist gerade die zweite Gruppe von Motiven (Punkte 3 und 4), die auf Verstärkung von Innovationen sowie auf einen breiteren Einsatz von KI, Big Data und Machine Learning zielen, im deutschen Sprachraum seit einigen Jahren besonders ausgeprägt. Dies erfordert eine weitergehende Analyse.

Innovationen, von denen hier die Rede ist, beziehen sich (und basieren) auf Wissenschaft und Technik, Forschung und Entwicklung – sowie auf deren Anwendung und Nutzung: es geht um die technowissenschaftliche Digitalisierung und Informatisierung. Vor diesem Hintergrund ist die damit verbundene Sichtweise auf Wissenschafts- und Technikentwicklung in

spätmodernen Wissensgesellschaften in den Blick zu nehmen.[15] Zunächst wäre daran zu erinnern, dass die Begriffskarriere von Datensouveränität eine (ex post) Reaktion auf wissenschaftlich-technische Entwicklungen darstellt – eine Entwicklung, die freilich verbunden ist mit ökonomischen, politischen und gesellschaftlichen Motiven. Es ist die Dynamik von Wissenschaft und Technik, genauer: von wissenschaftsbasierter Technik, die die spätmodernen Wissenschaftsgesellschaften herausfordert. Mit anderen Worten, es sind Entwicklungen von KI, Machine Learning, Big Data sowie der Rechner-, Sensor-, Speicher- und Netztechnologie der letzten 15 Jahre, die eine Veränderungen in allen gesellschaftlichen Bereichen wie auch der spätmodernen Wissenskultur induziert haben. Digitalisierung beschreibt wie kein anderer Begriff diese wissenschaftlich-technisch bedingte und erzeugte globale Transformation spätmoderner Wissensgesellschaften, was seit einigen Jahren als Megatrend bezeichnet wird. So kann man sagen: Dass heute allenthalben von Datensouveränität gesprochen wird, ist Folge und Produkt avancierter Wissenschafts- und Technikentwicklung – nicht im engen, technizistischen Sinne, sondern als Folge wissenschaftlicher und technischer Dynamiken.

Recht besehen bezieht sich der Such- und Sondierungsbegriff Datensouveränität damit auf die komplexen Verhältnisse Wissenschaft und Technik einerseits und Gesellschaft, Mensch, Wirtschaft, Politik und Recht andererseits. Nun brauchen die ausgeklügelten Modelle und philosophisch-soziologischen Binnendifferenzierungen der Verhältnisbestimmung hier nicht weiter interessieren. Relevant ist einzig die Sichtweise auf Wissenschaft und Technik im Rahmen des Gesellschaftlichen. Mit Datensouveränität tritt – zumindest im zweiten Motivtyp (Punkte 3 und 4) – ein wissenschaftlich-technologischer Fortschrittsoptimismus zu Tage, wie er sich bei den Abwehr- und Schutzmotiven (Punkte 1 und 2), hier insbesondere im Datenschutzdiskurs, kaum findet.

Der Fortschrittsoptimismus erstaunt angesichts der Wissenschafts- und Technikentwicklung des 20. Jahrhunderts. Spätestens seit der Atom- und Biotechnologie, eigentlich schon seit der Dampfmaschine und der Industrialisierung im 19. Jahrhundert, gehört die Wahrnehmung von Ambivalenzen von Wissenschaft und Technik zum Selbstverständnis moderner Gesellschaften. Noch im Katastrophenjahr 1986 (Tschernobyl, Sandoz, Chal-

15 Eine solche Grundlagenperspektive wird im üblichen Diskurs zu Datensouveränität kaum in Anschlag gebracht.

lenger) sprach Ulrich Beck zu recht von Risikogesellschaft und von reflexiver Moderne (Beck 1986). Institutionen und Verfahren der Technikfolgenabschätzung etablierten sich, um Wissenschafts- und Technikentwicklungen so zu gestalten, dass gesellschaftliche Risiken frühzeitig erkannt und minimiert werden (Grunwald 2002). Eine solche Sicht hinterfragt den modernen Fortschrittsoptimismus, der von Francis Bacon im frühen 17. Jahrhundert programmatisch entwickelt wurde, nämlich dass wissenschaftlich-technischer Fortschritt stets human-gesellschaftlichen Fortschritt impliziert – zumindest wenn man Technik »richtig« entwickelt und nutzt (vgl. Schmidt 2011). Gernot Böhme hat in den frühen 1990er Jahren treffend ein »Ende des Baconschen Zeitalters« (Böhme 1993) diagnostiziert. Von einem solchen Ende kann heute – angesichts der zweiten Diskurslinie um Datensouveränität (Punkte 3 und 4), die die Innovations- und Nutzensermöglichung so prominent in den Mittelpunkt stellt – keine Rede mehr sein. Vielmehr findet sich eine Renaissance des Bacon'schen Programms: Ambivalenzwahrnehmungen und Risikodiskurse vermisst man.

Wenn nun der Begriff Datensouveränität produktiv für eine aktuelle Wissenschafts- und Technikgestaltung und -regulation, nämlich die der Digitalisierung und Informatisierung in Anschlag gebracht und zu einem normativen Gestaltungskonzept ausgearbeitet werden soll, ist es also angezeigt, die offenkundigen Ambivalenzen ergänzend und kritisch in den Blick zu nehmen: Datensouveränität kann kein stromlinienförmiges Konzept eines affirmativen (wissenschaftlich-technologischen) Datensouveränitäts-Optimismus sein, das einseitig allein Innovationschancen anvisiert und der vermeintlich normativen Kraft des Faktischen über Sachzwang- und Anpassungsargumente hinterherläuft, sondern es muss Ambivalenzen und Risiken prospektiv und proaktiv als Gestaltungsherausforderungen für Gesellschaft, Politik und Mensch ansehen. Nur so kann das produktive, auf Gestaltung ausgerichtete Potenzial, welches der Begriff Datensouveränität (auch) in sich trägt, entwickelt und für die Praxis nutzbar gemacht werden. Dieses Potenzial soll im Folgenden am Beispiel eines (durchaus ebenfalls ambivalenten) Aspektes diskutiert werden.

## 6. Der Bürger, User und Konsument als souverän Handelnder: Ein mündiger und kritischer »Tanz auf des Messers Schneide« statt eines risikoaversiven Handlungsverzichts

Lässt man sich auf den Begriff Datensouveränität im Rahmen der zweiten Motivgruppe, also als Konzept zur Ermöglichung und Nutzung von Innovationen (positiv) ein, dann ist zunächst eine individualistische Perspektive (und eine entsprechende individualistische Engführung) unumgänglich. Was kann unter Datensouveränität des Users, Konsumenten oder Bürgers verstanden werden?

Als Einstiegsbedingung gilt, wie in vielen deutschsprachigen Papieren zu Digitalpolitik und zur Datensouveränität ausgeführt: Um die wissenschaftlich-technische Entwicklung vertieft(er) und weitreichend(er) nutzen zu können, bedarf es auf der Nutzerseite einer Modifikation der Haltungen und Handlungen, deutlicher: einer Anpassung. Es gelte, »Vertrauen«[16] in digitale Systeme, in Dateninfrastrukturen, Plattformbetreiber und Intermediäre zu entwickeln, wobei dieses Vertrauen nicht blind und naiv sein dürfe, sondern verbunden sein müsse mit individueller Datenkompetenz bzw. digitaler Mündigkeit. Ein grundlegendes Wissen ist für Datenkompetenz unumgänglich,[17] vor dessen Hintergrund der Nutzer entsprechend seiner Präferenzen und Zwecke hinreichend optimierend die jeweiligen Mittel wählt. Der Nutzer erscheint individualistisch weithin als rationaler *homo oeconomicus* und übernimmt als solcher Verantwortung für sein Handeln im digitalen Raum. Die Verpflichtung hierzu erscheint als andere Seite der Nutzungs- und Partizipationsoptionen bzw. der »Freiheit«, sich im digitalen Raum zu bewegen.

Beispielhaft für die individualistische Engführung von Datensouveränität ist die bereits erwähnte, von Unternehmensvertretern gegründete Arbeitsgruppe Innovativer Staat der Initiative D21 (Horn/Stecher 2019). Ihr Positionspapier weist dem Nutzer eine wesentliche Verantwortung zu

---

16 Der Begriff »Vertrauen« tritt in einigen Papieren auf, die Datensouveränität thematisieren, siehe Horn/Stecher 2019: 6, BMBF 2020: 12 oder Belko 2021: 15. Und auch in verwandten Papieren, etwa im Entwurf des europäischen Daten-Governance-Gesetzes (DGA) findet sich dieser psychologisch ausgerichtete Begriff, der durchaus individualistisch als (Technik-) Akzeptanzbeschaffung gedeutet werden kann.

17 Genannt werden Kompetenzen wie »technical literacy, privacy literacy, information literacy und civic literacy und […] resilience literacy und cultural literacy« (Belko 2021: 14).

und fordert von diesem »Datenkompetenz« ein.[18] Allgemein wird Datensouveränität hier als »Befähigung im Umgang mit den eigenen Daten« verstanden (ebd.: 4): »[D]er Begriff ›Datensouveränität‹ [stellt] die Autonomie des Datengebenden in den Mittelpunkt, welcher reflektiert und durch seine Fähigkeiten selbstständig in der Lage ist, sich informationell selbstbestimmt in der ›Daten-Welt‹ zu bewegen.« (ebd.) Somit geht es »um die Möglichkeit einer aktiven, selbstbestimmten Gestaltung der Lebenswelt unter der Nutzung digitaler Technologien.« (ebd.)

Mit anderen Worten und deutlicher auf den Einzelnen zugeschnitten:

> »Bei dem Autonomieprinzip, das dem Souveränitätsbegriff innewohnt, geht es also um die Souveränität des Individuums, sich und seine Umwelt nach eigener Vorstellung immer wieder neu zu ›entwerfen‹. Die Souveränität bedeutet, jederzeit die Hoheit und Verantwortung über den eigenen Lebensentwurf zu haben. Von dieser normativen Grundlage ausgehend kann die ›Datensouveränität‹ daher nichts anderes bedeuten, als Selbstbestimmung über das Daten-Abbild seines Selbst […].« (ebd.: 3)

Es wird, wie vorne erörtert, von »Freiheit«, »Freiheitschancen« und »Freiheitsrechten« gesprochen. Vor dem Hintergrund dieser individualistisch-liberalistischen Position vertritt die D21-Initiative einen (in der philosophischen Tradition etablierten) »Befähigungsansatz« (ebd.: 4). Der Bürger soll das normative Ziel der Datensouveränität »ermöglicht« werden durch »Befähigung«, also den »Erwerb von Kompetenzen im Bereich Datenschutz« (ebd.: 1, 6). Die Ermöglichungsbedingungen von Datensouveränität des Einzelnen liegen, so wird betont, sowohl bei den »NutzerInnen als datengebende Komponente, als auch [bei der] datenverwendende[n] Seite[n] – sprich d[en] Unternehmen – und [dem] Staat.« (ebd.: 4)

In eine ähnliche individualistische Richtung stößt die Stellungnahme des Ethikrates *Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung* von 2017. Allerdings geht es nicht um Datensouveränität allgemein, sondern diese bezieht sich auf den Gesundheitssektor. Datensouveränität wird als Leitbild im Horizont von »Freiheit« angesetzt, das positiv zu füllen und zu implementieren ist – und das mit individueller Verantwortungsübernahme verbunden ist. »Datensouveränität, verstanden als eine den Chancen und Risiken von Big Data angemessene verantwortliche informationelle Freiheitsgestaltung, sollte das zentrale ethische und

18 Auch wenn der Fokus wie oben beschrieben gewählt wird, finden sich auch Abschnitte zu neuen rechtlichen Rahmenbedingungen und neuen technischen Maßnahmen des Datenschutzes.

rechtliche Ziel im Umgang mit Big Data sein.« (Deutscher Ethikrat 2018: 252) Als grundlegend zur Erreichung dieses Ziels wird ein adäquates Wissen – als konstitutives Element für »Vertrauen« – angesehen, wie auch Belko (2021: 15) ausführt: »Um die Mündigkeit des Einzelnen zu stärken, sich innerhalb des Systems nicht zu verlieren, muss man Vertrauen durch Wissen schaffen.« Die Erlangung dieses Wissens und der entsprechenden wissensbasierten Kompetenzen erscheint nicht nur als notwendig, sondern auch als möglich.[19] Kritisch äußern sich Knorre u. a. (2020: 41) über das »neue Leitbild Datensouveränität«:

> »Aus einem [traditionellen] Abwehrmechanismus, nämlich einen rechtlichen Schutzbereich für den Nutzer zu schaffen, wird ein Gestaltungsanspruch in einem Hoheitsgebiet, auf dem er dank exzellent designter Bildungsangebote an der Weitergabe seiner Daten aktiv mitwirkt. Dies ist so gesehen eine Weiterentwicklung des Heldenbilds des rationalen Verbrauchers, der die ihm gegebenen Möglichkeiten im Sinne einer kritisch-reflektierten Entscheidung auch tatsächlich nutzt«.

Trotz aller notwendigen Skepsis und Kritik an der individualistischen Engführung eines rational handelnden Nutzers findet sich hier, implizit und etwas versteckt, ein weiterführendes und weitreichendes Gestaltungsverständnis, bzw. traditioneller gesprochen: ein anderes Steuerungskonzept. Dies kann an interessante Governancemodelle anschließen, etwa an Konzepte wie der dezentralen Kontextsteuerung.[20] Während traditionell, technisch oder systemtheoretisch gesprochen, eher das Bild des zentralen Top-Down-Akteurs im Sinne des »Totdämpfens von Störungen« oder Interventionen aller Art vorherrschte und damit eine verhindernd-konservative Risikoperspektive verfolgt wurde, findet sich hier so etwas wie das Bild des »Tanzes auf des Messers Schneide« als adaptives, flexibles, kontextsensitives Handeln sehr unterschiedlicher Akteure in einem komplexen Gegenstandsfeld.[21] Es geht hier um ein Eintauchen in den Datenstrom,[22] auf dem »zu tanzen« ist – einem Strom, der in seiner Dynamik und Komplexität, in seiner Zeitlichkeit und seinen Selbstorganisationsmechanismen

19 Offenbar wird angenommen, dass aus Notwendigkeit die Möglichkeit folgt.
20 Einiges geht auf Wilke (1983; 2007) zurück, siehe auch Benz u. a. 2007 und Heinelt 2018.
21 Bei Lüde u. a. 2009 findet sich dieser veränderte Governance- und Gestaltungsansatz – als Abkehr von traditionellen Steuerungskonzepten. Zur Metapher des »Tanzes auf des Messers Schneide« siehe Schmidt 2004 sowie Schmidt 2015: 29 f.
22 Zur treffenden Metapher des Stroms siehe Deutscher Ethikrat 2018: 40 und Knorre u. a. 2020: 41.

weithin opak und intransparent bleibt.[23] Was bleiben sollte, ist ein jeweils revidierbares Handeln unter Nichtwissen, Unsicherheit und Risiko.[24] Wer hinreichendes Wissen und entsprechende Kontrolle erwartet, kann nicht im Datenstrom dabei sein; statt dessen gilt es, Resilienz zu entwickeln,[25] um somit aufmerksam, umsichtig und kritisch im digitalen Raum partizipieren zu können. Man könnte gar von einer neuen individuellen Governanceform sprechen.[26] Diese (durchaus metaphorische) Sichtweise nimmt Anleihen aus den Struktur- und Systemwissenschaften auf, nämlich den Selbstorganisations- und Autopoiesistheorien, der Synergetik und Nichtlinearen Dynamik, den Chaos- und Katastrophentheorien; Ursprünge weisen bis in die Kybernetik und Informationstheorie zurück (vgl. Schmidt 2015).

## 7. Anknüpfungen zur Zuschreibung von »Souveränität« in der Lebenswelt

Mit diesem Bild eines adaptiv-flexiblen Handlungsverständnisses im Datenstrom sind Anknüpfungspunkte zum Begriff Souveränität in lebensweltlicher Zuschreibungspraxis gegeben. Vermutlich wurzelt hier ein ebenso verborgenes wie weiterführendes Spezifikum des deutschsprachigen Diskurses um Datensouveränität. Begrifflich ist nicht, wie historisch und staatsrechtlich, von *dem* Souverän die Rede. Vielmehr wird adjektivisch oder adverbial eine Handlung als »souverän« oder ein Akteur (i. A: rollen- und situationsspezifisch) als ein mit »Souveränität« Handelnder charakterisiert.[27] Mit dem Coach Stéphane Etrillard kann man sagen: »Eine weitere Bedeutung von Souveränität findet sich außerhalb der staatlich-politischen

23 Dabei gilt allgemein, dass durch KI und Big Data eine enorme Komplexität erzeugt wird, die grundlegend zu Anfragen von epistemischem Zugang hinterfragen. So ergibt sich schon aus wissenschaftlicher Perspektive eine Opazität, Intransparenz und Undurchsichtigkeit, die zu einem prinzipiellen Nicht-Wissen-Können führt, wie in Schmidt 2022 ausgeführt. Wenn schon Wissenschaften begrenzt sind, so ist diese Begrenzung noch stärker in Alltag und Lebenswelt, das heißt für den lebensweltlich Handelnden anzusehen.

24 Zum Begriff »Nichtwissen« sowie des Handelns unter Nichtwissen, siehe Böschen u. a. 2004 sowie, aus Perspektive der Technikfolgenabschätzung: Schmidt 2021.

25 Vgl. auch: Deutscher Ethikrat 2018: 192.

26 Damit zeigt sich womöglich eine Nähe zu Foucault.

27 Souveränität erscheint so primär ein zugeschriebener Handlungsbegriff. Ein solcher Zugang stellt, über die Begriffsgeschichte hinaus, eine weitere Basis für eine Begriffsexplikation dar, wie im Folgenden dargelegt wird.

Zusammenhänge: Sie betrifft die Persönlichkeit des Menschen und charakterisiert Souveränität als bestimmte Eigenschaft einer Person.« (Etrillard 2006: 13) Ob Souveränität, fast essentialistisch, als »Eigenschaft einer Person« oder besser rollen-, kontext- und situationsspezifisch zu fassen sein mag, sei dahingestellt. Doch Etrillard führt zu recht aus, dass Souveränität im Alltag zugeschrieben wird – und zwar in einer »Welt«, die von »Komplexität«, das heißt von »Vielfalt, Unvorhersagbarkeit, Wandel, Bewegung, Vernetzung und Wechselwirkung« (Etrillard 2006: 14) geprägt ist. Einige wenige Beispiele sollen genügen.

Zunächst ist es nicht unüblich, von souveränen Dozierenden, Lehrer:innen, Hochschullehrer:innen oder auch souveränen Redner:innen zu sprechen. Zur rollenspezifischen Zuschreibung von Souveränität ist, über das Fachwissen hinaus, die Handlungskompetenzen der Dozentin in der Interaktion mit Studierenden oder Schüler:innen entscheidend (vgl. Neuenschwander 2006). Allgemein sind für Lehr-Lern-Prozesse an Schule und Hochschule Regeln und Konventionen vorgegeben, die Dozierende kaum verändern können. Mit den Regeln sind Machtasymmetrien zwischen Dozierenden und Studierenden verbunden: Dozierende haben Möglichkeiten der Sanktionierung. Nun würde man einen Dozenten, der bei kleinsten Störungen sofort machtförmig einschreitet und Studierende von der Vorlesung ausschließt, nicht als souverän – sondern als autoritär, als streng, als hysterisch-überreagierend oder gar als unsicher-kontrollorientiert – bezeichnen. Als souverän gilt eine Dozierende dann, wenn sie gelassen, flexibel, adaptiv und (das heißt: auch) lässig mit Störungssituationen umgeht, es gleichzeitig jedoch vermag, die Störung zu reduzieren oder zu unterbinden. Sie hat (qua Rolle) Autorität, Handlungskompetenz, Machtmöglichkeit und Kontrolloption in diesem durch allgemeine Regeln gegebenen Setting, aber sie setzt diese nur moderat und mit Augenmaß zielführend ein. Würde sie allzu massiv intervenieren, würde sie die Studierenden einschüchtern und Lehr-Lern-Prozesse erschweren. Souverän zu handeln meint, klug abzuwägen und die Tugend der Mäßigung und Verhältnismäßigkeit zu praktizieren, das heißt nicht alle Machtmöglichkeiten einzusetzen, sondern situationsspezifisch einen »flexiblen Tanz auf des Messers Schneide« vorzunehmen zwischen Reduktion der Störungen und Herstellung von Ruhe einerseits und Ermöglichung eines lebendigen und motivierenden Lernprozesses

andererseits.[28] Das heißt Souveränität basiert auf Handlungs- und Kontrollmacht, jedoch wird auf machtförmige Handlungen situativ verzichtet – zugunsten der Ermöglichung von intendierten Prozessen. Diese Polarität scheint für ein aktuelles Datensouveränitätsverständnis genuin.

Zwei weitere Beispiele der alltäglichen Verwendungspraxis des Souveränitätsbegriffs sind naheliegend. Strukturell verwandt zum souveränen Handeln des Dozenten ist das, was als »souveränes Spiel« einer Fußballmannschaft bezeichnet wird. Dabei ist nicht der Sieg oder die Anzahl der Tore souverän, sondern die Spielhandlungen, die zu dem Sieg geführt haben. Die Höhe des Sieges ist nicht entscheidend; man kann sogar sagen, dass wenn eine Mannschaft hoch gewonnen hat, dies zwar den Gegner deklassiert haben mag, aber keiner besonderen Handlungen, also gar keine Souveränität bedurfte. Nur bei einem Gegner, der stark und unberechenbar ist, kann man Souveränität zeigen. Souveränität meint also (analog zu obigem Beispiel) nicht umfassende Machtausübung, sondern kluger und dosierter Machteinsatz – und damit partieller Machtverzicht. Gerade der Verzicht, Macht umfassend einzusetzen und Kontrolle total zu realisieren, rückt Souveränität in Richtung einer Tugend.[29]

Auch Handlungen von Autofahrer:innen werden gelegentlich als »souverän« bezeichnet. Das Fahren im Straßenverkehr ist einerseits ein stark regelbasiertes Handeln. Andererseits hat der Autofahrer Handlungsfreiheiten, etwa was Ziele, Wege, Geschwindigkeit, Fahrstil und Nutzungsformen angeht – anders als ein Lokführer. Eine Autofahrerin, die gehetzt mit größtmöglicher Geschwindigkeit und in kürzester Zeit ans Ziel kommt, bezeichnet man nicht als souverän. Vielmehr gilt eine Autofahrerin als souverän, wenn sie sich nicht aus der Ruhe bringen lässt, wenn sie gelassen bleibt, umsichtig und verantwortungsbewusst handelt – und sich in den Verkehrsstrom einfügt.[30] Wer souverän fährt, hat ein Tacit Knowledge,

---

28 Markus Neuenschwander beschreibt die »souveräne Lehrperson« wie folgt: »Eine souveräne Klassenführung ist mit besonders hohen Anforderungen an die Lehrpersonen verbunden. Einerseits erfordert eine hohe Flexibilität von den Lehrpersonen die Fähigkeiten, Unterrichtssituationen präzis zu diagnostizieren und kommunikativ geschickt vorzugehen. Andererseits setzt die Regelorientierung das Wissen um eine effiziente Klassenführung voraus, so dass günstige Regeln vorgeschlagen und durchgesetzt werden können.« (Neuenschwander 2006: 245).

29 Womöglich finden sich Überschneidungen zu tugendethischen Grundhaltungen – und allgemein zu dem, was seit einigen Jahrzehnten als »Tugendethik« bezeichnet wird.

30 Die Metaphern »Verkehrsstrom« und »Datenstrom« zeigen die deutliche Nähe dieses Begriffsfeldes.

also ein geübtes Sensitivitätswissen, welches er sich im Handlungsvollzug angeeignet hat und welches handlungsleitend ist.

Es gibt ferner Beispiele, die zeigen, dass nicht in allen Handlungsfeldern Souveränität zugeschrieben wird. Es ist unüblich, davon zu sprechen, dass jemand souverän seine Steuererklärung erstellt – man hat hier zu wenig Handlungsoptionen. Die Erstellung ist stark von Randbedingungen präformiert und von rechtlichen Erfordernissen determiniert. Komplementär liegen die Dinge bei Künstlern, bei denen in der üblichen Sichtweise kaum einschränkende Bedingungen vorliegen. Es gibt wenig Regeln – das künstlerische Handeln ist weithin offen. Diese Offenheit steht der Redeweise eines souveränen Handelns des Künstlers entgegen. – Zusammengenommen, weder im Fall der weitgehenden Fremdbestimmung (z. B. Steuererklärung) noch der vollständigen Autarkie (z. B. freies künstlerisches Schaffen) wird im Alltag üblicherweise Souveränität zugeschrieben.

Die Beispiele der lebensweltlichen Zuschreibungspraxis des Begriffs »souverän« lassen sich bündeln. Ein souveränes Handeln ist durch mindestens folgende Elemente zu kennzeichnen: (a) In dem Handlungsfeld, in dem ein souveränes Handeln eines Akteurs zugeschrieben wird, gibt es Regeln, die allerdings nicht jedes Handeln vollständig determinieren: Souveränität ist ohne regulierte Rahmenbedingungen – als reine Autarkie – nicht möglich. (b) Vielmehr können im Rahmen gegebener Regeln unterschiedliche Handlung gewählt werden: Souveränität ist nur dort möglich, wo Handlungsalternativen realisiert werden können und in diesem Sinne eine Freiheit – und keine Fremdbestimmung – gegeben ist oder ermöglicht wird.[31] (c) Souveränes Handeln bedarf eines hinreichenden kognitiven und praktischen Wissens und entsprechender Kompetenzen im Handlungsfeld: Souveränität ist Wissens- und Kompetenz-basiert. (d) Innerhalb des gegebenen Handlungsfeldes hat der souverän Handelnde eine hinreichend umfassende Handlungsmacht, durch welche er das Handlungsfeld (zumindest partiell) kontrollieren kann bzw. könnte. Der Handelnde setzt diese Handlungsmacht im praktischen Vollzug nicht vollumfänglich ein: Souveränität ist stets verbunden mit einem gewissen Handlungsverzicht und einer Ab- und Aufgabe von Kontrolle, um damit Ziele zu realisieren und Zwecke

31 An dieser Stelle kann nur angedeutet werden, dass somit eine Nähe des Begriffs »Souveränität« zu jenem der »Autonomie« gegeben ist. Dieser Zusammenhang wird unter anderem im bereits angesprochenen Papier der D21-Initiative hergestellt (Horn/Stecher 2019).

zu verfolgen bzw. weil die Kosten (z. B. zeitlicher Art) zu groß sind, um die Handlungsmacht vollumfänglich zu realisieren.

## 8. Fazit: Die Gestaltungsherausforderungen annehmen und nutzen

Die aktuelle Digitalpolitik hat den Begriff Datensouveränität gerade im deutschen Sprachraum zu einem Fokus des Diskurses über die digitale Zukunft der Gegenwartsgesellschaft gemacht. Das Bild des flexibel-adaptiven »Tanzes auf des Messers Schneide« vor dem Hintergrund ermöglichender Regulierungen, das in diesem Beitrag in perspektivischer Absicht mit dem Begriff in Verbindung gebracht werden kann, eröffnet neue Horizonte, über individuelle wie politisch-gesellschaftliche Gestaltung von Zukunftstechnologien nachzudenken – und neue Gestaltungs- und Governance-Modelle zu entwickeln. Dies gilt auch eingedenk der eigenartigen technikoptimistischen Ambivalenz des Begriffs Datensouveränität. Dass eine rein individualistische Perspektive zu kurz greift, sollte deutlich geworden sein. Aber auch eine rein staatliche und regulatorische Perspektive ist nicht hinreichend, ja kann nicht mehr greifen, weil wissenschaftlich-technische Entwicklungen der Digitalisierung und Informatisierung so ubiquitär und medial vorangeschritten sind. So regt der Begriff Datensouveränität an, neu und anders, grundlegender und kritischer zu denken – auch was die Überschreitung individualistischer wie staatlich-regulatorischer Zugänge angeht. Die Herstellung und Sicherung von Datensouveränität sowie die Einübung und Kompetenzentwicklung eines datensouveränen Handelns stellt eine gesellschaftliche Querschnittsherausforderung dar. Sie ist als dezidiert politisch zu bezeichnen – politisch bedeutsam für den Einzelnen, für Staat und Politik, für Wirtschaft sowie für Wissenschaft und Technik.

# Datensouveränität durch Dateninfrastrukturen: Das Leuchtturmprojekt Gaia-X

*Christian Person und Moritz Schütrumpf*

Digitale Souveränität und Datensouveränität kursieren als Schlagwörter bereits seit längerer Zeit, obgleich die Begrifflichkeiten bis heute keine einhellig anerkannte Konturierung erfahren haben. Popularität erlangten beide Begriffe allerdings vor allem durch den gerade in Europa immer lauter werdenden Ruf der Politik nach digitaler Souveränität in und für Europa, allen voran seitens des deutschen Bundeswirtschaftsministeriums (BMWi 2016: 33 f.).

Der Wunsch nach mehr Souveränität im digitalen Raum in Europa ergibt sich dabei vor allem durch die schier übermächtigen Positionen vornehmlich amerikanischer oder chinesischer Konzerne im Digitalsektor. Durch die marktbeherrschenden Stellungen dieser *Hyperscaler* sind die Bürgerinnen und Bürger sowie die Unternehmen Europas in eine große Abhängigkeit von deren Technologien und Infrastrukturen geraten. Transparenz sowie Vertrauen sind Mangelware und europäischen Datenschutzregeln droht eine permanente Unterwanderung.[1] Unter diesen Rahmenbedingungen ist an den selbstbestimmten Aufbau datengetriebener Ökosysteme, gar einer europäischen Datenwirtschaft, frei vom Einfluss außereuropäischer Akteure, kaum zu denken (BMWi 2019: 8). Der hohe ökonomische und gesellschaftliche Wert, den die Nutzung großer Datenmengen als Ressource verspricht, kann somit aktuell von europäischen Unternehmen und Institutionen nicht realisiert werden, was einerseits in einem erheblichen Innovationsdefizit

1 Beispielhaft sei der US-amerikanische Cloud Act genannt, welcher amerikanische Clouddienstleister dazu verpflichtet, den US-Behörden Zugriff auf die Daten ihrer Nutzerinnen und Nutzer zu verschaffen, selbst wenn diese außerhalb der USA gespeichert werden. Europäische Bürgerinnen und Bürger sowie Unternehmen, die amerikanische Clouddiensteanbieter nutzen, haben entsprechend keine Kontrolle und Transparenz darüber, wer Zugriff auf ihre Daten bekommt. Hinzu kommt, dass etlichen amerikanischen Anbietern vorgeworfen wird, die gesammelten Geschäftsdaten ihrer Kundinnen und Kunden zu eigenen Zwecken zu gebrauchen (vgl. FAZ: 2020).

und fehlender Partizipation an den Vorteilen der Datenwirtschaft resultiert, andererseits aber auch die Frage aufwirft, welche Rolle dem Individuum in der modernen Datenwirtschaft noch zukommt.

Die deutsche und europäische Antwort auf die geschilderte Lage waren zunächst hohe und umfangreiche Anforderungen an den Datenschutz, insbesondere im Hinblick auf personenbezogene Daten, um einen effektiveren Grundrechtsschutz des Individuums zu gewährleisten (vgl. Europäische Kommission 2020a: 4). Für Wirtschaft und Wissenschaft stellt der Datenschutz allerdings neben den bereits erwähnten Abhängigkeiten bisweilen eine weitere Hürde für eigene datenbezogene Vorhaben dar, was ihre Innovationsfähigkeit zusätzlich hemmt. Nicht ohne Grund wird der Wunsch lauter, dass sich das Datenschutzrecht von einer »bürokratischen Innovationsbremse« zu einem »Innovationskatalysator« entwickeln solle (Seidel/Seidel 2020: 609).

Datenschutz allein scheint freilich nicht die adäquate Antwort, wenn es darum geht, wirtschaftliche und technologische Abhängigkeiten sowie Innovationsdefizite zu adressieren. Zunehmend tritt daher die Forderung nach Datensouveränität neben den Datenschutz, teilweise auch explizit als Gegenentwurf zu diesem.[2]

So heißt es beispielsweise 2016 in der Digital-Strategie des Bundeswirtschaftsministeriums:

»Wir müssen eine auf gemeinsamen Grundsätzen (zum Beispiel Datensicherheit und Datensouveränität) beruhende europäische Daten-Standortpolitik entwickeln.« (BMWi 2016: 25) sowie »Die Regulierung muss Investitionen und Innovationen ermöglichen, den Missbrauch marktmächtiger Strukturen verhindern, *Datensouveränität der Verbraucherinnen und Verbraucher* sichern und ein offenes Internet garantieren.« (BMWi 2016: 8, unsere Hervorhebung, CP/MS)

Es galt somit aus politischer Sicht, eine Antwort auf die Frage zu finden, auf welche Art und Weise mehr Datensouveränität innerhalb von Europa verwirklicht werden kann. Sichtbar wird dies anhand aktueller Gesetzesvorhaben auf europäischer Ebene, insbesondere dem geplanten Data Act (2022) sowie dem Data Governance Act (2022), welche beide Ausflüsse der Europäischen Datenstrategie sind (Europäische Kommission 2020a: 14 ff.).

2 Beispielsweise forderte 2016 der damalige Bundeswirtschaftsminister Sigmar Gabriel auf seiner Eröffnungsrede des 9. Nationalen IT-Gipfels ein Umdenken im Umgang mit Daten, weg vom klassischen Datenschutz hin zur Stärkung der Datensouveränität (Gabriel 2016).

Von diesen Gesetzesvorhaben erhofft man sich, dass insbesondere die Datenwirtschaft in legislativer Hinsicht ausreichend adressiert wird, um einen Innovationsschub für Europa zu initiieren (Europäische Kommission 2022a).[3] Dass es hiermit aus politischer Sicht für eine innovative Datenwirtschaft nicht getan ist, zeigen sowohl die Datenstrategien der Bundesregierung als auch die der Europäischen Kommission, denn im Vordergrund stehen hier neben den genannten legislativen Vorhaben vor allem die Schaffung von Dateninfrastrukturen und Datenräumen als notwendige Voraussetzung einer florierenden souveränen europäischen Datenwirtschaft.[4]

Sind die Ziele »Datensouveränität« durch »Dateninfrastrukturen und Datenräume« benannt, stellt sich unweigerlich die Frage, »Wie wollen wir dies erreichen?« (Bundesregierung 2021a: 12). Eine Antwort auf diese Frage soll das Projekt Gaia-X geben, welches zum Ziel hat, diese bestehende Lücke auszufüllen. Nicht ohne Grund wurde es entsprechend von der Bundesregierung in diesem Zusammenhang als erste und auch wichtigste Maßnahme genannt (Bundesregierung 2021a: 12).

Die Aufgabe, der sich dieser Beitrag im Rahmen des vorliegenden Sammelbandes widmet, ist es daher, nach einer kurzen Vorstellung des Projekts Gaia-X (1.) und der Darstellung der wissenschaftlichen Debatte zum Konzept Datensouveränität (2.) zu erfragen und zu erörtern, welchem Begriffsverständnis innerhalb des Gaia-X-Projekts gefolgt wird (3.) und welche Rückschlüsse sich hieraus für künftige Debatten ziehen lassen (4.).

## 1. Vorstellung der Entwicklung von Gaia-X

Der Startschuss für das Projekt Gaia-X fiel auf dem Digital-Gipfel 2019 in Dortmund. Ursprünglich vom Bundeswirtschaftsministerium konzipiert, mündete es in ein vitales, deutsch-französisches Kooperationsprojekt (BMWi 2020a), dem sich schon bald weitere europäische Staaten anschließen sollten. Vorangetrieben und entwickelt wird das Projekt mittlerweile von

3 Beispielsweise heißt es in ErwG. 1 des Entwurfes des Data Act: »High quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth.«

4 Die Ausgestaltung »leistungsfähiger« und »nachhaltiger« Dateninfrastrukturen wird von der Bundesregierung in ihrer Datenstrategie 2021 als »Fundament« für Innovation in der Datenökonomie genannt (Bundesregierung 2021a: 10 ff.).

mehr als 2500 Beteiligten von über 300 Unternehmen und Organisationen, inzwischen sogar über die Grenzen von Europa hinaus.[5] Bewusst nicht genannt ist die Politik, denn nach dem durch das deutsche und französische Wirtschaftsministerium erfolgten Start der Initiative hat sich die politische Administration bewusst aus der aktiven Mitgestaltung des Projekts herausgezogen und nimmt mittlerweile vor allem die Rolle eines Förderers ein.[6] Das Projekt wird allerdings nach wie vor eng begleitet, gerade um auch legislative Lücken frühzeitig zu identifizieren. Grundsätzlich ist das Projekt dezentral organisiert, mit in über 15 europäischen Ländern verteilten *Hubs*. Um dem Projekt einen gemeinsamen Koordinator und ein Sprachrohr nach außen zu geben, wurde im Jahr 2020 die Gaia-X European Association for Data and Cloud AISBL (Gaia-X AISBL) gegründet, in der sich alle Beteiligten aktiv beteiligen können und welche die zentralen Vorgaben des Projekts im engen Austausch mit der Community nach einem *bottom-up*-Prinzip erarbeitet. Die Gaia-X AISBL veröffentlicht hierzu insbesondere verschiedene konzeptionelle Papiere zur Konkretisierung der Vorgaben (einen Überblick über das Projekt bieten Person/Schütrumpf 2022).

Es ist, wie bereits in den anfänglichen politischen Ankündigungen deutlich wurde, ein ambitioniertes Ziel, dem man sich mit Gaia-X verschrieben hat. So werden im *Visions & Strategy*-Papier der Gaia-X AISBL zehn Kernprinzipien genannt, denen das Projekt gerecht werden soll und welche die Ambitionen und Motivation des Projekts unterstreichen (Gaia-X AISBL 2021a). Souveränität ist hierbei zunächst einmal nur eines unter vielen Leitprinzipien. Und doch kommt der Souveränität in Gaia-X eine besondere Stellung zu, was von der Politik, aber auch seitens des Projekts immer wieder deutlich nach außen getragen wird. So widmen beispielsweise *Otto* und *Tardieu* (Mitglieder des *Board of Directors* der Gaia-X AISBL, eines der maßgeblichen Entscheidungsgremien innerhalb der Organisation) der digitalen Souveränität im Zusammenhang mit Gaia-X einen ganzen Artikel, in welchem sie die Rolle von Gaia-X für die Schaffung europäischer digitaler Souveränität herausstellen (Tardieu/Otto 2021: 99 f.). Auch das Bundeswirtschaftsministerium betont die Rolle von Souveränität, wenn es die Zielsetzung des Projekts auf der Webseite des Ministeriums wie folgt beschreibt:

5 So gibt es mittlerweile auch eine Interessensvertretung des Projekts (einen sogenannten *Hub*) in Südkorea.

6 Dies zeigt sich daran, dass in beiden Staaten Förderwettbewerbe stattfanden, um das Projekt voranzutreiben.

»Mit Gaia-X entwickeln Vertreterinnen und Vertreter aus Wirtschaft, Wissenschaft und Politik auf internationaler Ebene einen nachhaltigen Beitrag zur Gestaltung der nächsten Generation einer europäischen Dateninfrastruktur. Ziel ist eine sichere und vernetzte Dateninfrastruktur, *die den höchsten Ansprüchen an digitale Souveränität genügt* und Innovationen fördert.« (BMWK 2022, unsere Hervorhebung, CP/MS)

Gerade zu Beginn des Projekts blieb allerdings relativ unklar, was genau unter einer »sicheren und vernetzten Dateninfrastruktur« verstanden wird. Häufig war beispielsweise die Rede von Gaia-X als »europäische[r] Datencloud« (Benrath/Löhr 2021). Jedoch war die Schaffung einer »datensouveränen« Cloud für den europäischen Raum zu keinem Zeitpunkt tatsächlich das Ziel des Projekts. *Otto/Burmann* beschreiben eine Dateninfrastruktur wie folgt:

»Eine Dateninfrastruktur stellt für einen bestimmten Gesellschaftsbereich wie die Mobilität oder für eine gesamte Volkswirtschaft Daten, Datendienste und Regeln für die Datennutzung für Individuen und Organisationen bereit. Durch die Nutzung der Dateninfrastruktur durch Datengebende, Datennutzende sowie Intermediäre entstehen Datenräume. Dateninfrastrukturen bilden die informationstechnische Basis für Datenräume.« (Otto/Burmann 2021: 284)

Mit einer Dateninfrastruktur ist ein viel grundlegenderes Ziel angestrebt als lediglich der Aufbau einer eigenen Cloud. Vielmehr geht es um die Schaffung einer standardisierten technologischen Infrastruktur für das Aufsetzen von Cloud-, Edge- und damit verbundenen Dienstleistungen. Dementsprechend ist es das Ziel des Gaia-X Projekts, gemeinsame Standards in Form von Software und Regeln nach festgelegten Leitprinzipien zu erarbeiten, die den eigenverantwortlichen Betrieb einer derartigen Dateninfrastruktur durch Unternehmen und Organisationen ermöglichen. Auf der offiziellen Projektseite der Gaia-X AISBL wird zwischen folgenden Standards unterschieden (vgl. Gaia-X AISBL 2021 g):

– *Regulatory Standards*: in einer bestimmten Rechtsordnung festgelegte rechtliche und regulatorische Standards
– *Industry specific Standards*: branchenspezifische Standards und Konformitätsregeln
– *Technical Standards*: branchenübergreifende Standardisierung technischer Bausteine

Durch diese Standardisierung erhofft man sich, Monopolstrukturen aufzubrechen, Lock-In-Effekte zu überwinden und so die Abhängigkeiten von au-

ßereuropäischen Akteuren zu reduzieren und »die *digitale Souveränität* der Nachfrager von Cloud-Dienstleistungen als auch die Skalierungsfähigkeit und Wettbewerbsposition europäischer Cloud-Anbieter« zu stärken (BMWi 2019: 11, unsere Hervorhebung, CP/MS).

## 2. Das Konzept der Datensouveränität aus wissenschaftlicher Perspektive – ein schillernder Begriff

Sowohl im wissenschaftlichen als auch im politischen und medialen Diskurs über die digitale Transformation der Gesellschaft hat sich der Begriff der Souveränität zu einem Leitkonzept entwickelt. Forderungen nach Daten-, digitaler, technologischer oder virtueller Souveränität sind allgegenwärtig und gehören zum Standardrepertoire der Debatte. Die inflationäre Verwendung der Begrifflichkeit Souveränität im Kontext der Digitalisierung geht jedoch mit dem Problem einher, dass der Souveränitätsbegriff sehr unterschiedlich gebraucht wird. Eine einheitliche Begriffsverwendung ist nicht erkennbar, da mit dem Begriff unterschiedliche Konnotationen, Ansprüche und Zielsetzungen verknüpft werden (Hummel u. a. 2021a: 1). Dies gilt insbesondere für das Konzept der *Daten*souveränität, das bei einer intensiveren Auseinandersetzung mit der wissenschaftlichen Literatur als vielschichtig, facettenreich und komplex erscheint. Die Literatur ist gekennzeichnet durch ein unklares, mehrdeutiges Begriffsverständnis, da das Konzept unterschiedlich definiert und angewendet wird, mithin ein »begriffsgeschichtliches und diskurspolitisches Chamäleon« (Gehring 2021: 2) darstellt.

Um diesbezüglich mit linguistischen Mitteln Ordnung in das terminologische Chaos zu bringen, untersuchen Hummel u. a. (2021b) im Rahmen einer systematischen Literaturanalyse, wie unterschiedlich der Begriff Datensouveränität in der einschlägigen Forschungsliteratur verwendet wird und arbeiten Differenzen in Bezug auf Begriffsverständnis, Adressaten, Kontext, normative Ansprüche und Herausforderungen heraus. Dadurch gelingt es ihnen nicht nur, die Mehrdimensionalität und Komplexität des Konzepts zu verdeutlichen, sondern auch die »Bandbreite an unterschiedlichen Akteuren zu Tage [zu fördern], die in verschiedenen Kontexten Anspruch auf Datensouveränität erheben und ihr dabei unterschiedliche Ausdrucksformen (Datensouveränität als Recht/als Befähigung/als technische Designentscheidung) zuschreiben« (Beise/Eckes 2021). Auf dieser Basis

entwickeln sie anschließend ein Kriterien-Raster, mit dessen Hilfe man sich dem Konzept Datensouveränität analytisch annähern und unterschiedliche Begriffsverständnisse systematisieren kann (siehe Tabelle 1).

| **Analysekategorie** | **Leitfrage** | **Beispiele** |
|---|---|---|
| Akteure | Wer ist Adressat? | Konsumenten, Staaten, ethnische Gruppen, Gesellschaft |
| Kontext | In welchem größeren Zusammenhang wird Souveränität verhandelt? | Gesetzgebung, IT-Architektur, Forschung |
| Werte | Mit welchen Werten wird Souveränität in Verbindung gebracht? | Kontrolle und Macht, Privatheit, Deliberation und Inklusion |
| Deskription | Was ist der primäre Fokus? | Rechte / Ansprüche, Fähigkeiten / Kompetenzen, Rechtskonzept |
| Herausforderungen | Was sind die zentralen Hindernisse? | Natur der Daten, technische Hindernisse, Komplexität |
| Handlungsstrategien | Wie sollen Herausforderungen bzw. Hindernisse adressiert werden? | Regulierung, Rechtsinnovation, technisches Design, Befähigung und Bewusstsein (*awareness*) |

Tabelle 1: Konzeptionelles Analyseraster zum Vergleich unterschiedlicher Begriffsverständnisse von Datensouveränität
*Quelle: eigene Darstellung in Anlehnung an Hummel u. a. 2021b*

Schon was unter dem Begriff der Datensouveränität verstanden wird und worauf der primäre Fokus des Konzepts liegt, ist in der Literatur umstritten. Datensouveränität wird je nach Autor als Recht und Anspruch, als Fähigkeit oder als Ergebnis von Gesetzgebungsprozessen verstanden. Außerdem wird das Verhältnis zwischen Souveränität im Allgemeinen und Datensouveränität im Speziellen thematisiert: Ist Datensouveränität lediglich Bestandteil einer allgemeineren Form von Souveränität oder ein eigenständiges Konzept, gar deren Voraussetzung? Darüber hinaus werden auch unterschiedliche Herausforderungen benannt, die mit dem Konzept verbunden sind. Diese können aus der Natur von Daten und ihren spezifischen Eigenschaften (in Abgrenzung zu anderen Arten von Ressourcen und materiellen Gütern), aus technischen Designs und IT-Ar-

chitekturen, unvollständigen oder asymmetrischen Informationen sowie unklarer Rechtslage resultieren. Des Weiteren werden unterschiedliche Handlungsstrategien diskutiert, um Datensouveränität zu erhalten bzw. zu erreichen. Hierzu gehören beispielsweise technologische, regulatorische und rechtliche Innovationen, aber auch die Vermittlung spezifischer Fähigkeiten und Kompetenzen (z. B. *data literacy*) oder die Schaffung von Aufmerksamkeit (*awareness*) für die Konsequenzen fehlender Datensouveränität. In Bezug auf die Regelungsadressaten wird deutlich, dass sehr unterschiedliche Handlungssubjekte Anspruch auf Datensouveränität erheben und somit Bezugspunkt von Datensouveränität sein können: dies reicht von einzelnen Individuen in ihrer Rolle als Bürger, User und Konsument, über Organisationen (privatrechtliche, öffentliche/staatliche oder Nichtregierungs-Organisationen) bis hin zu Kollektiven unterschiedlichster Form (Populationen, Staaten, Gesellschaften). Auch die Kontexte, in denen Datensouveränität verhandelt wird, variieren: Sie umfassen beispielsweise die Gestaltung von IT-Systemen, die Gesetzgebung, aber auch die Forschung oder den gesellschaftlichen Diskurs allgemein. Schließlich wird der Begriff mit unterschiedlichsten normativen Konzepten aufgeladen und in Verbindung gebracht. So werden in Bezug zu Datensouveränität unterschiedliche Werte thematisiert wie Macht und Kontrolle, Privatheit, Eigentum, Deliberation, aber auch Inklusion und Partizipation. Datensouveränität kann entweder diese Werte fördern oder durch Beachtung und Verfolgung dieser Werte verwirklicht werden (Hummel u. a. 2021b).

Eine Gemeinsamkeit weist jedoch die Mehrzahl der Studien auf: Souveränität impliziert stets Ansprüche auf Macht und Kontrolle. Datensouveränität wäre insofern die Kontrolle über die eigenen Daten. Individuelle oder kollektive Akteure sind diesem Verständnis nach datensouverän, »wenn sie zur Ausübung von Kontrollansprüchen rund um die Verwendung sie betreffender Daten befähigt sind« (Hummel u. a. 2021a: 3). Datensouveränität bezeichnet somit »die Fähigkeit einer juristischen oder natürlichen Person zur Selbstbestimmung über ihre Datengüter« (Otto/Burmann 2021: 284). Der Begriff umfasst demzufolge die Kontrolle von Akteuren über Datenzugriff und -verarbeitung, das heißt wer Zugriff auf die eigenen Daten hat, wie und von wem diese für welche Zwecke verarbeitet werden und wie sich dieser Datenzugriff bzw. diese Datenverarbeitung auf den eigenen Freiheitsvollzug auswirkt. Der einzelne Akteur muss selbstbestimmt über den Umgang mit persönlichen Daten und die Verwendung der ihn betreffenden Daten im Rahmen der Datenwirtschaft bestimmen können. Dieses

Verständnis wirft jedoch die provokante Frage auf, ob Souveränität »auch die bewusste Entscheidung gegen Kontrolle, ja gar den souveränen Kontrollverlust [umfasst]? Und müsste das zuweilen als paternalistisch gescholtene Datenschutzrecht demnach nicht an die Grenze seiner Leistungsfähigkeit geraten, weil es genau diesen Kontrollverlust nicht zulassen könne?« (Beise/Eckes 2021).

Insofern kann es nicht überraschen, dass mit Blick auf das einzelne Individuum das Konzept der Datensouveränität von Datenschützern kritisch gesehen und ein Spannungsverhältnis zwischen Datenschutz und Datensouveränität konstatiert wird. Freilich muss man das Konzept der Datensouveränität nicht als pauschale Abkehr vom klassischen Datenschutzgedanken und dem Recht auf informationelle Selbstbestimmung verstehen, sondern kann es auch als dessen kontextabhängige Fortentwicklung unter Big Data-Bedingungen hin zu einem Instrument der informationellen Freiheitsgestaltung betrachten (Hummel u. a. 2021a: 5–6). In diesem Sinne zeichnet sich Datensouveränität durch zwei zentrale Aspekte aus. Analog zum klassischen Datenschutz weist das Konzept zunächst eine abwehrrechtliche Dimension auf, da der Schutz von Persönlichkeitsrechten und die Bewahrung individueller Freiheitsvollzüge gewährleistet werden soll. Auch im Kontext von Big Data sollen Individuen ausreichende Kontrolle über ihre Daten haben, um ihre Privatsphäre schützen und personenbezogene Daten gegenüber externen Zugriffen abschirmen zu können. Allerdings bleibt das Konzept nicht bei einem bloßen Ausschlussrecht stehen, sondern geht über das Recht auf informationelle Selbstbestimmung hinaus und zeichnet sich durch positiv-partizipative Ansprüche aus. Handlungssubjekte sollen in die Lage versetzt werden, eigene Daten verfügbar zu machen und somit selbstbestimmt über die Verwendbarkeit der eigenen Daten entscheiden zu können. Individuen sollen befähigt werden, eine sachgerechte, wohlinformierte und selbstbestimmte Abwägung zwischen diesen beiden Aspekten vorzunehmen und eine angemessene Balance zwischen Schutz/Abschirmung und kontrollierter Bereitstellung der eigenen Daten zu erzielen und gleichzeitig durch die Bereitstellung personenbezogener Daten (z. B. in Form von Datenspenden) für spezifische Verwendungszwecke an datengetriebenen Koordinations-, Erkenntnis- und Innovationsprozessen partizipieren zu können (Hummel u. a. 2021a: 7–11). In einer positiven Sichtweise fungiert Datensouveränität somit als »Chiffre für die Rückgewinnung von Handlungs- und Verfügungsmacht im digitalen Raum« (Gehring 2021: 3), da das Konzept über den bloßen Schutzgedanken hinausgeht und konkrete

Gestaltungsansprüche, mithin ein *Empowerment* der Handlungssubjekte, impliziert.

Während die Literaturanalyse von Hummel u. a. (2021b) das große Verdienst aufweist, einen signifikanten Beitrag zur Klärung des Konzepts Datensouveränität zu leisten, liegt der Fokus der Analyse auf der wissenschaftlichen Debatte. Die Autoren merken selbstkritisch an, dass man diese Thematik auch in anderen Kontexten analysieren müsste: »First, its scope is limited insofar as it focuses on academic writing. It would be interesting to extend similar analyses of data sovereignty to other fields, such as journalism and social media content« (Hummel u. a. 2021b: 14). Des Weiteren verdeutlicht die Studie, dass mit Blick auf die Handlungssubjekte der Fokus auf der Individualebene oder der Kollektivebene liegt, das heißt Datensouveränität wird häufig aus der Sicht einzelner Individuen in ihren unterschiedlichen Rollen (Bürger, Konsument, User) oder aus Sicht von Populationen und Staaten diskutiert. Die organisationale Ebene als Bezugspunkt für Datensouveränität, insbesondere die unternehmerische Perspektive, scheint diesbezüglich vernachlässigt zu werden. Diese beiden Aspekte sollen im Folgenden adressiert werden.

## 3. Die (Daten-)Souveränität aus Sicht von Gaia-X

### 3.1 Digitale Souveränität als Datensouveränität und Cloudsouveränität

Digitale Souveränität – Cloudsouveränität – Datensouveränität. Die wenig trennscharfe, aber gleichzeitig beinahe inflationäre Begriffsverwendung, gerade wenn es um die Adressierung politischer Ziele geht, ist Thema vieler Beiträge dieses Bandes. Zu Recht wird davor gewarnt, dass Datensouveränität nicht zu einem bloßen *buzzword* oder *catch-all-term* verkommen sollte (Beise/Eckes 2021). Gaia-X sticht nun dadurch hervor, dass das Projekt klar formuliert, was in seinem Kontext unter digitaler Souveränität verstanden wird. Die Relevanz des hierbei entstehenden Konsenses ist dabei keineswegs zu ignorieren, denn er spiegelt das geteilte Verständnis aller beteiligter Unternehmen und Organisationen inklusive der involvierten Politik wider.

Zunächst einmal wird ganz allgemein unter Souveränität die Fähigkeit zur Ausübung von Selbstbestimmung verstanden. Deutlich wird hierbei hervorgehoben, dass damit weder ein politisches noch ökonomisches Verständnis von Souveränität adressiert sein soll (Gaia-X AISBL 2021a: 3). Entspre-

chend grenzt sich das Projekt bereits von den Wirrungen rund um das allgemeine Verständnis von Souveränität ab.[7] Insbesondere ist es kein staatsrechtlich geprägtes Verständnis, sondern zielt zunächst einmal auf die Souveränität von Akteuren im privaten Raum ab. Hinzu kommt, dass der Begriff Souveränität allein in einen digitalen und technologischen Kontext gesetzt wird.[8]

Laut Glossar und im Übrigen bereits seit Beginn des Projekts (BMWi 2020b: 3) wird dabei unter *digitaler* Souveränität konkret folgendes verstanden:

> »Digital Sovereignty is the power to make decisions about how digital processes, infrastructures and the movement of data are structured, built and managed.« (Gaia-X AISBL 2021 f)

Digitale Souveränität wird hier entsprechend deutlich als Oberbegriff für verschiedene Anknüpfungspunkte verwendet. Datensouveränität wird dabei ausdrücklich als Teilaspekt der digitalen Souveränität verstanden (BMWi 2020b: 3), was sich so auch teilweise in der wissenschaftlichen Debatte widerspiegelt.[9] In der Gesamtschau der von der Gaia-X AISBL publizierten Dokumente nimmt Gaia-X dabei nicht nur die Datensouveränität ins Blickfeld, sondern es fällt zudem auch der Begriff der Cloudsouveränität oder auch der technologischen Souveränität (Gaia-X AISBL 2021b: 8). Im Gegensatz zur Datensouveränität erfährt dieser Begriff zumindest in den offiziellen Dokumenten zwar keine klare, ausdrückliche Konturierung wie etwa die (Daten-)Souveränität, doch kann er in der Gesamtschau der Ziele von Gaia-X zumindest näher bestimmt werden. Denn werden die Probleme mit der Verwendung und Teilung von Daten ausgeblendet, bleiben davon abgesehen insbesondere die Probleme mit der benannten technologischen Abhängigkeit von ausländischen Akteuren. Entsprechend wird die technologische Souveränität durch die Kernprinzipien »Fair« und »Frei« adressiert, wonach zum einen Fairness unabhängig von der zugrundeliegenden Technologie gewährleistet werden soll. Zum anderen wird aufgrund der Open-Source-Basis technologischen Lock-in-Effekten vorgebeugt und auf dieser

---

7 Vgl. zur grundlegenden Debatte insbesondere den Beitrag von Tim Eckes in diesem Band.

8 »Gaia-X does not provide any political or economic interpretation of sovereignty, but instead provides a framework to configure sovereignty from a digital and technical perspective.« (Gaia-X AISBL 2021a: 3).

9 Vgl. den Beitrag von Gehring in diesem Band.

Basis eine selbstbestimmte Umsetzung der eigenen individuellen Geschäftsmodelle ermöglicht (Gaia-X AISBL 2021a: 3 f.).

Ziel des Projekts ist entsprechend sowohl die Umsetzung der Daten- als auch der technologischen Souveränität. Für die Zwecke dieses Beitrags soll aufgrund der zugrundeliegenden Thematik des Sammelbands allerdings ein Fokus auf die Datensouveränität im Sinne von Gaia-X gelegt werden. Entsprechend werden im Folgenden bewusst keine näheren Ausführungen zur technologischen oder allgemein der digitalen Souveränität erfolgen, wenngleich beide Teilaspekte digitaler Souveränität in der Umsetzung von Gaia-X durchaus gewisse Schnittmengen haben.

### 3.2. Datensouveränität – Erklärtes Ziel der Gaia-X-Initiative

Bereits bei der ersten Vorstellung 2019 wurde die Herstellung von Datensouveränität im europäischen Raum als klares Ziel benannt, was im Sinne des damaligen Wirtschaftsministeriums der »vollständige(n) Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf« entsprach (BMWi 2019: 6 f.). Und diese Zielsetzung hat nach wie vor Bestand. Allein der Begriff Datensouveränität fällt in den offiziellen, seitens der Gaia-X AISBL mittlerweile veröffentlichten Dokumenten bezüglich der Ausgestaltung der geplanten Standards und Rahmenregelwerke beinahe inflationär mit fast 60 Nennungen. Auch auf der offiziellen Seite der deutschen Repräsentation von Gaia-X durch das BMWK findet sich dieser Gedanke wieder, wonach die Kontrolle über Daten im Zentrum des Begriffs der Datensouveränität steht:

> »Unternehmen sowie Nutzerinnen und Nutzer sollen Daten sammeln und miteinander teilen – und zwar so, dass sie darüber die Kontrolle behalten. Sie selbst sollen festlegen, was mit ihren Daten passiert und wo sie gespeichert werden, so dass in jedem Fall die Datensouveränität gewährleistet ist.« (BMWK 2022)

Die Definition des Bundeswirtschaftsministeriums blieb infolge der Entwicklung des Projekts dabei beinahe unangetastet. So wird »Souveränität über Daten« von der Gaia-X AISBL mittlerweile in gleicher Stoßrichtung als *»Participants can retain absolute control and transparency over what happens to their data.«* (Gaia-X AISBL 2021b: 11) definiert. Insofern knüpft das Projekt Gaia-X an die gängige Gemeinsamkeit aller Datensouveränitätsdebatten an: Macht und Kontrolle über Daten.

Entsprechend des Definitionsansatzes muss daher nochmals differenziert werden. Einerseits soll den Teilnehmern vermittelt werden, dass sie die Entscheidungsgewalt über ihre Daten behalten. Andererseits geht es auch um einen transparenten Prozess, damit die Teilnehmer überhaupt in die Lage versetzt werden, ihre Entscheidungsgewalt auch selbstbestimmt ausüben zu können.

Doch wer kommt als Adressat der Datensouveränität im Sinne von Gaia-X in Betracht? Spannend ist diese Frage vor allem deshalb, da gerade zu Beginn des Projekts beispielsweise durch das Bundeswirtschaftsministerium Gaia-X noch als Instrument zur Sicherung der Datensouveränität »aller europäischer Bürgerinnen und Bürger und der Unternehmen« ins Feld geführt wurde (BMWi 2020c: 14 f.). Deutlich wird zunächst, dass der Datensouveränität im Sinne von Gaia-X kein staatsbezogenes Verständnis zugrunde liegt. Eine Adressierung entlang des ursprünglich vom Bundeswirtschaftsministerium vorgelegten Begriffsverständnisses lässt sich mittlerweile aber jedenfalls auch nicht mehr ohne Weiteres begründen, wenn ein genauerer Blick auf das Wording der Gaia-X AISBL geworfen wird. Denn primär soll den Teilnehmern (*Participants*) Kontrolle und Transparenz bezüglich ihrer Daten ermöglicht werden. Ein Blick in das Konzeptmodell[10] von Gaia-X verrät dabei, dass als Teilnehmer nur Akteure innerhalb von Gaia-X verstanden werden. Dies exkludiert zunächst einmal die Endnutzer, die außerhalb des Scopes von Gaia-X stehen. Es schließt zudem aber auch mögliche Ressourceninhaber[11]– also letztendlich potenzielle Dateninhaber – aus, denn Anbieter und Ressourceninhaber müssen nach dem Verständnis von Gaia-X nicht zwingend deckungsgleich sein und es wird häufig vorkommen, dass der Ressourceninhaber nicht direkt innerhalb eines Gaia-X-konformen Datenökosystems akkreditiert ist, gerade wenn personenbezogene Daten Gegenstand der Dienstleistung sind. Das Gaia-X Konzeptmodell sieht dabei selbstverständlich vor, dass der Anbieter vom Ressourceninhaber rechtlich auch zur Nutzung der Ressourcen ermächtigt wurde. Bislang ist allerdings nicht ersichtlich, wie diese Beziehung rechtlich oder technisch durch Gaia-X abgesichert werden wird bzw. überhaupt werden soll.

10 Das Konzeptmodell ist einsehbar im Architektur Dokument der Gaia-X AISBL (Gaia-X AISBL 2021b: 14).

11 Der Ressourcenbegriff ist innerhalb von Gaia-X weit gedacht und erfasst sowohl Datenbestände als auch Software oder sogenannte Knotenpunkte (Gaia-X AISBL 2021b: 17).

Dass der Endnutzer nicht primär erfasst ist von Gaia-X, ist dabei kein Geheimnis. Der Befund deckt sich mit anderen projektbezogenen Publikationen, bei denen der Endnutzer aus projektseitiger Perspektive ebenfalls nicht als Zielgruppe genannt wird. Dieser sei allerdings durch die Leitprinzipien von Gaia-X berücksichtigt, gar in das Zentrum der Überlegungen gestellt (BMWi 2020d: 8). Impliziert werden könnte damit, dass die gestärkte Datensouveränität der Unternehmen auch in einer verbesserten Stellung der Datensouveränität der Bürgerinnen und Bürger bei der Nutzung der Servicedienstleistungen der Unternehmen resultieren würde. Ob dies tatsächlich in gleicher Weise wie für die Stellung der Unternehmen der Fall sein wird, ist allerdings in jedem Fall kritisch zu hinterfragen und wird in dieser Form auch in den aktuellen Publikationen der Gaia-X AISBL nicht vertreten. Die Aussage des Bundeswirtschaftsministeriums zielte wohl eher darauf ab, dass die Datensouveränität der Bürgerinnen und Bürger mittelbar dadurch gefördert wird, dass diese durch die hohen Anforderungen an Transparenz und Vertrauen ebenfalls in ihrer Position gestärkt werden, wenn sie einen Gaia-X-konformen Dienst nutzen. Nicht zugestimmt werden kann dabei der Aussage, die Bürgerinnen und Bürger seien durch die Leitprinzipien in das Zentrum aller Überlegungen gestellt worden, jedenfalls wenn es um die Suche nach den Adressaten der Datensouveränität geht. Zu deutlich sind hierfür die Definitionsansätze der Gaia-X AISBL, die immer wieder den Teilnehmer von Gaia-X in das Zentrum der Datensouveränität rücken.

### 3.3 Datensouveränität – Und wie?

Zusammenfassend lässt sich der Datensouveränitätsbegriff von Gaia-X entsprechend definieren als »*Kontrolle* und *Transparenz* aller *Teilnehmer* hinsichtlich ihrer Daten«. Ist das Ziel in Form von »Kontrolle und Transparenz« als maßgebliche Kriterien für Datensouveränität aus projektseitiger Sicht somit ausgemacht, stellt sich anschließend die Frage, wie dieses Ziel nun durch die geplante Standardisierung umgesetzt werden wird. Vermittelt Gaia-X tatsächlich ihre Form von Datensouveränität oder wirbt die Initiative mit einer Eigenschaft, die sie gar nicht zu erfüllen vermag?

### *a) Regel- und Label-Rahmenwerk*

Grundsätzlich gibt es zunächst ein selbstregulatorisches Rahmenregelwerk, die sog. *Policy Rules*, dessen Anforderungen alle Teilnehmer von Gaia-X erfüllen müssen, was insbesondere die Anbieter von Cloud-Dienstleistungen innerhalb von Gaia-X betrifft. Die *Policy Rules* enthalten dabei insbesondere ein Bekenntnis zum Europäischen Datenschutz, treffen aber auch ansonsten transparenzbezogene oder vertragliche Anforderungen, die über das herkömmliche gesetzliche Niveau etwa der DSGVO hinausgehen. Kontrolle und Transparenz wird hierbei aus verschiedenen Blickrichtungen adressiert. Beispielsweise müssen Serverstandorte offengelegt werden, wodurch Datengeber in die Lage versetzt werden, zu bestimmen, wo und unter welcher Jurisdiktion ihre Daten gespeichert und verarbeitet werden (Gaia-X AISBL 2021c: 3). Hinzu kommt, dass die europäischen Regelungen beispielsweise zur Portabilität von Daten durch das Rahmenregelwerk adressiert werden, wodurch diesen auch dann zur Geltung verholfen wird, wenn ihr räumlicher Anwendungsbereich grundsätzlich nicht erfüllt wäre. Je nach Level (hierzu sogleich) müssen die Serviceanbieter auch Wahlmöglichkeiten für die Nutzer vorsehen, wie die Rechtswahl zugunsten eines Mitgliedstaats der EU oder die Möglichkeit auszuschließen, dass der Anbieter Zugriff auf Kundendaten erhält (Gaia-X AISBL 2021c: 5). Selbstverständlich adressiert Gaia-X mit ihrem Rahmenregelwerk, wie auch mit den sonstigen Standards, nicht ausschließlich die Datensouveränität, sondern auch Aspekte wie Sicherheit und Offenheit (Gaia-X AISBL 2021c: 3). Bereits anhand der *Policy Rules* lässt sich allerdings das Ziel entnehmen, die Position der Nutzer von Servicedienstleistungen durch Gaia-X erheblich zu verbessern, auch hinsichtlich Kontrolle und Transparenz. Denn obliegt es beispielsweise aktuell der Kontrolle der Serviceanbieter, wo Daten gespeichert werden, wird diese Kontrolle den Anbietern durch Gaia-X in gewissem Maß entzogen oder zwingt diese zumindest zu Transparenz und wird so wieder auf den Nutzer verlagert.

Um das so Erreichte zudem auch nach außen tragen zu können, wird ein Zertifizierungssystem für die von den Anbietern beworbenen Services in Form von Labels (aktuell Level 1 bis 3) eingeführt, sodass für jeden Teilnehmer von Gaia-X, aber auch für potenzielle, außerhalb des Gaia-X-Kosmos stehende Endnutzer (beispielsweise Verbraucher), ersichtlich ist, welche Standards an Sicherheit, Datenschutz, Portabilität und Transparenz ein Service erfüllt (Gaia-X AISBL 2021d: 2). Auch das Label-Rahmenwerk trägt

daher zur Transparenz der Servicedienstleistungen bei. Es ermöglicht, dass die Nutzer in die Lage versetzt werden, selbstbestimmte Wahlmöglichkeiten bezüglich ihrer Daten zu treffen.

### *b) Technische Implementierung*

Darüber hinaus setzt die Gaia-X-Initiative für ihren Ansatz zur Verwirklichung ihrer – sehr ambitionierten – Ziele vor allem darauf, dass die von ihr gewollten Prinzipien technisch durch Standardisierung in Form von Open-Source-Software umgesetzt werden, sodass Konzepte wie Datensouveränität nicht nur rechtlich, sondern vielmehr technisch und weitgehend automatisiert implementiert werden können (Gaia-X AISBL 2021b: 11).[12] Im Ergebnis könnte daher auch von »data sovereignty by design« gesprochen werden. Die technische Verankerung hat dabei einerseits den Vorteil, einen effektiveren Schutz von Daten vor missbräuchlicher Nutzung zu bieten, da auch die Durchsetzung von Vereinbarungen automatisiert erfolgt. Andererseits ist hierdurch gewährleistet, dass eine technische Umgehung der Datensouveränität bereits *qua* Design ausgeschlossen werden kann. Dies verbessert die Position der Datengeber ungemein, denn ein großes »Aber« bei der Teilung von Daten ist fehlendes Vertrauen in den Datennutzer, gerade bei sensiblen Daten. Eine rein rechtliche Lösung, beispielsweise im Rahmen der Vertragsgestaltung, verbessert die Position des Datengebers lediglich *ex post*, also nachdem es bereits zu einer abredewidrigen Datennutzung gekommen ist. Gerade für sensible Daten, beispielsweise Geschäftsgeheimnisse oder auch personenbezogene Daten, ist dies für viele Unternehmern nicht ausreichend, weshalb sich viele gegen eine Teilung von Daten entscheiden, was in gewisser Weise auch zu einer erheblichen Begrenzung eines souveränen selbstbestimmten Umgangs mit den Daten führt. Der vor allem technisch ausgelegte Lösungsansatz von Gaia-X soll dagegen bereits durch die technisch implementierte Vorbeugung etwaiger abredewidriger Datennutzungen eine Absicherung der Position des Datengebers *ex ante* ermöglichen, um so das Vertrauen des Datengebers zu stärken.

Doch wie bildet sich die technische Standardisierung nun konkret ab? Dies soll exemplarisch anhand der sogenannten *Federation Services* vorgestellt

---

12 »This document […] emphasizes a general ›compliance-by-design‹ and ›continuous-auditability‹ approach.«

werden. Die *Federation Services* sind eine Gaia-X-konforme Referenzarchitektur, bei deren Entwicklung auf Open-Source-Basis sich jeder Interessent beteiligen und später auch nutzen kann. Eine Nutzung der *Federation Services* ist später zwar wohl nicht konstitutiv für ein Gaia-X-Label, zeigt allerdings exemplarisch aufgrund der engen Zusammenarbeit bei der Entwicklung mit der Gaia-X AISBL bereits, welchen Anforderungen die Software künftiger Teilnehmer für Gaia-X jedenfalls gerecht werden müsste.[13] Aktuell befinden sich dabei vor allem vier Services in der Entwicklung: ein *Identity and Trust Service*, ein *Federated Catalogue*, das *Compliance Framework* und die sogenannten *Data Sovereignty Services* (Gaia-X AISBL 2021e: 5).

Die Palette der Vehikel, derer man sich bedient, um diese technische Implementierung zu vollziehen, ist entsprechend breit und soll an dieser Stelle nicht *en détail* aufbereitet werden. Darzustellen lohnen sich allerdings die *Data Sovereignty Services*, denn diese haben, wie bereits unschwer am Namen zu erkennen ist, im Kontext der Datensouveränität ein hohes Maß an Relevanz und verdeutlichen das zuvor geäußerte Verständnis davon, wer im Kontext von Gaia-X primärer Adressat von Datensouveränität ist. Bereits die grundlegende Beschreibung der *Data Sovereignty Services* lässt den ersten Schluss zu, wonach es vor allem einen Austausch von Daten verschiedener, durchaus auch mehrerer, Institutionen ermöglichen soll (Datentransaktion):

> »Data Sovereignty Services enable the sovereign data exchange of Participants by providing a Data Agreement Service and a Data Logging Service to enable the enforcement of Policies.« (Gaia-X AISBL 2021b: 39)

Anknüpfend an die projekteigene Definition der Datensouveränität, wird die Aufgabe der *Data Sovereignty Services* dabei konkret damit beschrieben, jedem Teilnehmer die volle Selbstbestimmung (Kontrolle und Transparenz) über den Austausch und das Teilen von (seinen) Daten zu geben, wobei die Funktionen der Services die Zeit vor, während und nach der Datentransaktion betreffen sollen (Gaia-X AISBL 2021b: 53 f.). Die Besonderheit ist dabei, dass die gesamte Datentransaktion auf technischer Ebene transparent abgebildet werden soll. Durch den Service *Data Contract Transaction (DCT)* soll beispielsweise der gesamte zugrundeliegende Vertrag technisch validiert

13 Sie werden beispielsweise von der Gaia-X AISBL als »Toolbox« für das Minimum an technischen Anforderungen für künftige Gaia-X-konforme Datenökosysteme bezeichnet (Gaia-X AISBL 2021e: 4). Aktuell befinden sich die *Federation Services* in der Entwicklungsphase und können noch nicht praktisch erprobt werden.

werden können, womit auch eine automatisierte Durchsetzung des Vertrags verbunden sein könnte (sogenannter Smart Contract), aber auch je nach Transaktion Datennutzungsregelungen (sogenannte *Usage Policies)* seitens des Datengebers vorgegeben und implementiert werden können (Gaia-X AISBL 2021b: 18). Intendiert ist zudem, diesen Service durch den Service *Data Exchange Logging (DEL)* zu flankieren, dessen Aufgabe darin bestehen soll, die gesamte Datentransaktion zu protokollieren und möglichst transparent für alle Beteiligten zu machen, was insbesondere Nachweise zur Klärung operativer Fragen liefern soll und so beispielsweise regelwidriger oder gar betrügerischer Nutzung der Daten vorbeugen kann (Gaia-X AISBL 2021e: 7).

Welche Schlussfolgerungen lassen sich nunmehr für die Entwicklung der Datensouveränität unter dem Mantel des Projekts Gaia-X schlussfolgern? Was Datensouveränität vor allem ausmacht und bislang in diesem Beitrag noch kaum zur Geltung kam, ist die bislang klaffende Lücke bezüglich einer vertrauenswürdigen Dateninfrastruktur, die es *allen* Teilnehmenden in gleichberechtigter Art und Weise ermöglicht, nicht wie aktuell im Verhältnis zu den großen *Hyperscalern*, überhaupt einen souveränen Umgang mit ihren Daten auszuüben. Gaia-X will entsprechend aus unternehmerischer Perspektive überhaupt erst einen souveränen Umgang mit den eigenen Daten ermöglichen, bei dem keine Abhängigkeit vom Serviceanbieter besteht, sondern eine echte Wahl möglich ist, was mit den Daten passiert und wo die Daten gespeichert werden. Darüber hinaus liegt der Beitrag von Gaia-X darin, dass durch die Transparenz des Vorgangs die Beteiligten vor einem Missbrauch ihrer Daten entgegen der gewünschten Nutzungsart geschützt werden. Kombiniert mit der forcierten Automatisierung bietet das Konzept daher tatsächlich eine digitale Umgebung, in welcher jedenfalls die Beteiligten in ihrer Datensouveränität maßgeblich unterstützt werden.

### 3.4 Einordnung in das Analyseraster von Hummel u. a. (2021b)

Welchen Mehrwert bietet die Betrachtung von Gaia-X nun für die Frage nach der Datensouveränität? Dies soll anhand der Einordnung des Datensouveränitätsverständnisses, welches sich anhand der Definitionen aber auch der Rahmenbedingungen und technischen Implementierungen ergibt, in das Analyseraster von Hummel u. a. (2021b) exemplifiziert werden.

Die erste Besonderheit ergibt sich bereits bei der Frage, wer überhaupt Adressat von Datensouveränität im Rahmen des Projektes ist. Gaia-X zielt in erster Linie nicht auf die Datensouveränität von Staaten oder einzelnen Individuen ab. Auch sind weder die Gesellschaft noch ethnische Gruppen Gegenstand der gewünschten Datensouveränität. Primäre Adressaten sind vielmehr ausschließlich die Teilnehmer von Gaia-X, entsprechend vor allem Unternehmen und Institutionen wie Forschungseinrichtungen, möglicherweise aber auch öffentlich-rechtliche Akteure. Diese werden von Gaia-X konkret benannt und profitieren auch in erster Linie von der geplanten Standardisierung der entstehenden Datenökosysteme. Deutlich wird dies insbesondere bei der Betrachtung der *Data Sovereignity Services*, welche die Datentransaktionen und damit die Beziehung von Serviceanbieter und Nutzer in den Vordergrund rückt, nicht dagegen das Verhältnis zum unter Umständen außerhalb des Konzepts stehenden rechtlichen Dateninhaber. Erst mittelbar verbessert Gaia-X aber auch den Status Quo außenstehender Akteure, wenn dies auch nicht ausdrücklich in den Projektdokumenten hervorgehoben wird. Nicht gemeint ist hiermit, dass die ermöglichte Datensouveränität der Unternehmen auf die Endnutzer durchschlägt, sondern dass durch die gesamten Rahmenbedingungen auch eine Verbesserung von deren Position einhergeht, beispielsweise durch die Transparenzanforderungen, aber auch durch die Durchsetzung des europäischen Datenschutzniveaus. Soweit Gaia-X seitens der Politik daher als Antwort für den Ruf nach europäischer Datensouveränität »aller europäischer Bürgerinnen und Bürger und der Unternehmen« ins Feld geführt wird (BMWi 2020c: 14 f.), sollte dies jedenfalls kritisch hinterfragt werden, was die Bürgerinnen und Bürger betrifft. Denn erkennbar ist die Zielsetzung von Gaia-X mittlerweile doch deutlich auf die Unternehmen oder andere beteiligte Organisationen gerichtet.

Der Kontext dieser organisationsbezogenen Datensouveränität ist dabei vor allem technischer Natur, sofern es um die Umsetzung geht. Daneben werden durchaus auch rechtliche Implikationen adressiert, beispielsweise durch die *Policy Rules*, aber auch im Rahmen der automatisierten Durchsetzung etwaiger Verträge. Durch die engen Verschränkungen zur Politik ist dabei durchaus auch die Gesetzgebung in die Prozesse involviert. Hinzu kommt, dass auch in wirtschaftlicher Hinsicht in verschiedenen Sektoren gearbeitet wird und so auch unterschiedlich hohe Anforderungen an die Datensouveränität je nach Branchengebiet adressiert werden können. Gleichermaßen kann Gaia-X auch im Kontext der Forschung einen erheblichen

Mehrwert bieten. Von daher steht die Datensouveränität von Gaia-X mit mehreren Ebenen im Zusammenhang und muss auch entsprechend diskutiert werden. Diese bestehenden Interpendenzen zwischen verschiedenen Ebenen, gerade hinsichtlich der technischen und rechtlichen Implikationen des Projekts, sorgen letzten Endes aber dann auch für eine erfolgreiche Umsetzung der Datensouveränität.

Die Werte, die Gaia-X mitbringt, sind dabei entsprechend der eigenen Definitionsansätze schnell gefunden, denn Selbstbestimmung in Form von Kontrolle und Transparenz ist, wie hier herausgearbeitet wurde, das Leitthema für die Umsetzung der Datensouveränität in Gaia-X. Selbstbestimmung geht dabei notwendigerweise einher mit Unabhängigkeit und Autonomie von anderen Akteuren. Bei näherer Auseinandersetzung ergibt sich allerdings eine weitere Differenzierung, denn gerade die Analyse der technischen Implementierung macht deutlich, dass Datensouveränität im Sinne von Gaia-X insbesondere zwei Aspekte von Kontrolle bezüglich Daten erfasst:

1. Kontrolle darüber, zu welchem Zweck die Daten genutzt werden dürfen.
2. Kontrolle darüber, wo die Daten gespeichert sind bzw. verarbeitet werden.

Die Herausforderungen, derer sich das Projekt annimmt, sind entsprechend vielfältig und komplex. Aufgrund der Ambition, für verschiedenste Sektoren einen branchenübergreifenden Mehrwert zu bieten, ist das zentrale Hindernis für das Vorhaben wohl seine Komplexität allein aufgrund der Vielzahl an beteiligten Stakeholdern. Hinsichtlich der Datensouveränität bleibt diesbezüglich vor allem die Frage offen, ob die technische Umsetzung ihren eigenen Anforderungen gerecht wird. Ob dies ausreichend ist, den erhofften Innovationsschub für die Datenwirtschaft zu initiieren, bleibt allerdings abzuwarten, denn wie so häufig gilt es auch zu klären, ob die rechtlichen Rahmenbedingungen bereits das hergeben, was zur rechtlichen Umsetzung der bislang vor allem technischen Konzepte notwendig ist. Jedenfalls durch die enge Einbindung der Politik, mittlerweile auch der Europäischen Union, scheinen allerdings auch diese Hürden zumindest überwindbar.

Zusammenfassend gesprochen adressiert Gaia-X vor allem eine Form von Datensouveränität, die einen wirtschaftlichen und letzten Endes unternehmerischen Umgang mit Daten ermöglicht. Diese Form »unternehmerischer« Datensouveränität, die vor allem dazu dient, datenbasierte Geschäftsmodelle umsetzen zu können, könnte tatsächlich als Innovati-

onskatalysator für die Herausbildung einer europäischen Datenwirtschaft wirksam werden.

## 4. Gaia-X – Zwischen unternehmerischer Datensouveränität und Datenschutz: Fazit

Inwiefern Gaia-X nun einen Beitrag für das allgemeine Begriffsverständnis von Datensouveränität leistet, bleibt abzuwarten. Es ist selbstverständlich aber auch nicht das Ziel von Gaia-X und dem vorliegenden Beitrag, das Begriffsverständnis rund um die digitale Souveränität aufzuklären. Gaia-X versteht sich selbst eher als Ermöglicher von Datensouveränität im Sinne des eigenen Begriffsverständnis und macht es sich in der Weise gewissermaßen auch einfacher, mit den Begrifflichkeiten umzugehen, wobei »einfacher« keineswegs negativ konnotiert sein soll, sondern in dem Zusammenhang eine Klarheit birgt, welche die wissenschaftliche Debatte teilweise missen lässt. Denn was Gaia-X begriffstechnisch ausmacht, ist ein relativ geradliniges Konzept von Datensouveränität.

Gaia-X wirbt dabei offensiv damit, Datensouveränität im europäischen Raum tatsächlich herzustellen. Wird dies allerdings unter die Semantik von Gaia-X subsumiert, dient es primär der Herstellung von Datensouveränität innerhalb von Gaia-X, letzten Endes entsprechend den Unternehmen, die Gaia-X nutzen werden, um ihre Geschäftsmodelle umzusetzen. Deutlich wird dies nach Ansicht der Autoren bei der Frage nach den Adressaten der Datensouveränität. Diese sind im Rahmen von Gaia-X primär die beteiligten Unternehmen und Organisationen innerhalb von Gaia-X. Nur mittelbar trägt das Projekt auch zur Verbesserung des Status von Endnutzern bei. Keine Adressaten des zugrundeliegenden Verständnisses sind Staaten als solche, was bereits durch die fehlende Anknüpfung an ein staatsrechtlich orientiertes Begriffsverständnis deutlich wird. Diese Adressierung ist selbstverständlich projektbezogen und nicht verallgemeinerungsfähig. Im Positiven könnte allerdings geschlussfolgert werden, dass Gaia-X, unabhängig von der Adressierung, beschreibt, was aus unternehmerischer Sicht Datensouveränität bedeutet und was für eine Umsetzung notwendig wäre, letztlich eine Form von »unternehmerischer« Datensouveränität vermitteln möchte.

Gaia-X könnte abseits von der Frage nach der Bedeutung von Datensouveränität ein weiterer großer Wurf gelingen, welcher in diesem Beitrag

bereits angedeutet wurde, denn Gaia-X adressiert neben der Datensouveränität vor allem auch den Datenschutz. Wie aus der bisherigen Beleuchtung der Debatte bereits hervorgegangen ist, sind Datenschutz und Datensouveränität komplementär zueinander, werden teils aber auch als konträre Konzepte aufgefasst. Gaia-X macht es sich entsprechend zum Ziel, beide Seiten der Medaille zueinander zu bringen, sodass es den Teilnehmern einerseits ermöglicht wird, ihre Datensouveränität aktiv dahingehend wahrnehmen zu können, ihre und die Daten anderer Teilnehmer nutzen zu können, ohne sich andererseits in einen Widerspruch zum hohen europäischen Datenschutzniveau begeben zu müssen.[14] Es ist daher nicht nur der Anspruch von Gaia-X, datenschutzkonforme oder datensouveräne Standards zu entwickeln. Anknüpfend an Hummel u. a. (2021a) tritt neben die negativ-protektive Funktion (Abwehrfunktion) der Datensouveränität daher vor allem auch die positiv-partizipatorische Funktion (Ermöglichungsfunktion) in den Vordergrund, wobei Adressaten nicht wie bei Hummel u. a. diskutiert einzelne Individuen wären, sondern die Unternehmen (2021b: 7–11). Es geht daher bei Gaia-X auch darum, neben den Aspekten Kontrolle und Transparenz als notwendige Grundlage für Datensouveränität eine rechtskonforme Datennutzung und -teilung zu ermöglichen, dies dann gewissermaßen als Form einer konstruktiven Datensouveränität.

14 Boris Otto hebt beispielsweise in einem Interview hervor, dass Gaia-X dazu diene, einen Ausgleich zwischen Datenschutz und Datennutz zu erzielen (vgl. Otto 2022).

# Datentoxikalität: Eine technikethische Herausforderung

*Gerhard Schreiber*

Im biochemischen Kontext wird als toxisch[1] die schädigende Wirkung eines Stoffes bei Kontakt mit einem biologischen System (Mensch, Tier, Pflanze) bezeichnet. Als Weiterführung dieser naturwissenschaftlichen Verwendungsweise von »toxisch« bzw. »Toxizität« zur Beschreibung des Ausmaßes der Giftwirkung eines bestimmten Stoffes auf lebende Organismen wird »toxisch« seit einiger Zeit vermehrt auch auf destruktive Denk- und Verhaltensweisen bezogen, die das gemeinschaftliche oder gesellschaftliche Miteinander von Menschen vergiften (z. B. »toxische Männlichkeit«[2]). Der Begriff wird auch auf alles Mögliche übertragen, was mit Risiko und/oder Dysfunktionalität behaftet sein und negative Auswirkungen zeitigen kann (z. B. toxische Wertpapiere, toxische Beziehungen, toxisches Arbeitsumfeld bis hin zur zwanghaft optimistischen toxischen Positivität). Insofern wird durch den in diesem Beitrag zur Diskussion gestellten Begriff der Datentoxikalität die Erweiterung des Bedeutungsspektrums von »Toxizität« fortgesetzt und zugleich spezifiziert, indem mit der Rede von »toxikalisch« bzw. »Toxikalität«[3] anstelle von toxisch bzw. Toxizität speziell auf die sozialpsychologische Dimension einer Schädigungswirkung abgehoben wird, wie sie auf der Ebene zwischenmenschlicher Beziehungen und in Prozessen sozialer Interaktion zur Geltung kommt. Über Phänomene toxischer Wirkung auf pharmakologischer, biochemischer, genetischer, physikalischer oder physiologischer Ebene hinaus soll durch die Rede von der Toxikalität von

---

1 Eine Adjektivbildung zu griechisch τοξικόν, »Gift zum Bestreichen der Pfeilspitzen«, kurz: »Pfeilgift«; aus griechisch τοξικός, »zu Pfeil und Bogen gehörig« (Passow 1825: 876; Kluge 2011: 923).

2 Vgl. auch die althergebrachten Bezeichnungen eines boshaft-gehässigen Menschen als Giftzwerg, Giftnudel oder Giftkröte.

3 Zu dieser Begriffsneuschöpfung vgl. Gennermann 2020, die unter Toxikalität nicht nur als giftig empfundene und beschreibbare physikalische und chemische Wirkungen, sondern auch entsprechende »zwischenmenschliche oder interinstitutionelle Beziehungen« ([2]) subsumiert.

Daten[4] also deren mögliche Schädigungswirkung im Bereich menschlichen Zusammenlebens in den Begriff gebracht werden.

Bevor ausgewählte Beispiele für Datentoxikalität dargestellt und technikethische Überlegungen darüber angestellt werden, wie einer derartigen Schädigungswirkung von Daten begegnet werden könnte, gilt es den Aspekt der Schädigung zu konkretisieren.

## 1. Schädigung

Unter Schädigung[5] ist sowohl der Prozess des Geschädigt*werdens* als auch der Zustand des Geschädigt*seins* zu verstehen, wobei der zugefügte bzw. erlittene »Schaden« eine »negative, beeinträchtigende Einwirkung *und* das [umfasst], was sie an Verlust, Zerstörung oder Nachteil zur Folge hat« (Pfeifer 1989: 1486; meine Hervorhebung, GS). Schädigung meint also nicht allein den schädigenden Vorgang selbst, sondern auch das weite Spektrum möglicher sich dadurch unmittelbar oder mittelbar einstellender Folgen. Jedwede negative Einwirkung als Schädigung verstehen zu wollen, hätte freilich einen völlig entkonkretisierten Schädigungsbegriffs zur Folge, dessen praktische Handhabbarkeit zu entgleiten drohte. In Anlehnung an den berühmten Satz des Paracelsus ist demnach zu statuieren: *dosis facit venenum* – die Dosis macht das Gift.[6]

4 Das Verhältnis von Daten und Informationen sei im Folgenden der Einfachheit halber im Anschluss an Bernhard C. Witt dahingehend gefasst, dass Daten »kontextfreie Angaben« sind, »die aus interpretierten Zeichen bzw. Signalen bestehen«, während Informationen »Daten« sind, »die (i.d.R. durch den Menschen) kontextbezogen interpretiert werden und (insbesondere prozesshaft) zu Erkenntnisgewinn führen« (Witt 2010: 4 f.). Daten sind also noch nicht, sondern werden erst zu Informationen durch Kontextualisierung und Interpretation – sie werden sozusagen in Form gebracht (so die eigentliche Bedeutung von lateinisch *informare* als einformen).

5 Ich spreche an dieser Stelle bewusst von Schädigung bzw. schädigend anstelle von Schädlichkeit bzw. schädlich, um den kleinen, aber bedeutsamen Unterschied zu markieren, dass etwas unmittelbar oder mittelbar *schädigend* wirken, während *schädlich* auch etwas sein kann, das *nicht* unweigerlich zum Eintritt einer unmittelbaren oder auch nur mittelbaren Schädigung führt. Die dem Adjektiv *schädlich* üblicherweise gegebene Bedeutung »zu Schädigungen führend« (Duden [6]2020: 720) ist also nicht im Sinne einer Zwangsläufigkeit zu verstehen, so wie das bloße Vorhandensein einer giftigen Substanz in einem lebenden Organismus nicht unbedingt zu einer Vergiftung desselben führt.

6 Im Original der *Septem Defensiones* (1537/1538) allerdings umgekehrt formuliert: »alle ding sind gift und nichts on gift; alein die dosis macht das ein ding kein gift ist« (Paracelsus 1928: 138).

Eine Schädigung liegt erst vor, wenn ein normativ definierter Schwellenwert – juristisch gesprochen: eine Erheblichkeitsschwelle – erreicht und überschritten wird (Meyer 2005: 36–39). Dies ist zweifellos bei zugefügten Verletzungen physischer oder psychischer Art der Fall, aber auch bei körperlich-seelisch-geistig sich auswirkenden Verletzungen individueller Freiheits- und Selbstbestimmungsrechte, die sich, sofern in ihnen ein Moment fremdmächtiger Willensdurchsetzung zum Tragen kommt, zugleich als *gewalthaltig* qualifizieren lassen (Schreiber 2022: 84–86). Eine Schädigungswirkung im strengen Sinne setzt also stets Urheberschaft voraus, welche sowohl personal wie nicht-personal, also subjektanalog (Gerhardt 1996: 8) gedacht werden und damit konkret identifizierbaren Personen ebenso wie Strukturen und Verhältnissen zukommen kann.

Als spezifische Form der Einwirkung ist Schädigung notwendig relational: Schädigung manifestiert sich stets im Verhältnis zu etwas oder jemandem, was nicht heißt, dass Schädigung von den sie Erleidenden immer auch *als* Schädigung wahrgenommen wird. Aus der Relationalität jeglichen Schädigungsgeschehens folgt deshalb, dass Schädigung *an sich* nicht existiert. Damit ist nicht behauptet, dass Schädigung immer auch von einem konkret identifizierbaren Subjekt gegenüber einem gleichermaßen konkret identifizierbaren Objekt erfolgt, wohl aber ist behauptet, dass es keine Schädigung ist, wenn sie in keiner Weise gegenüber etwas oder jemandem zur Wirkung kommt. Darin zeigt sich die pathische Seite einer Schädigungswirkung – pathisch entsprechend der Grundbedeutung von griechisch *πάσχειν* zunächst ganz allgemein als Erfahren einer Einwirkung von außen (Passow 1825: 399), noch ohne negative oder positive Bewertung, sodass das Feststellen einer Einwirkung und deren Bewertung zweierlei bleiben.

Mit der wesenhaften Relationalität von Schädigung korrespondiert der Umstand, dass die als Toxizität bezeichnete Schädigungswirkung eines bestimmten Stoffes auf der biochemischen Ebene dessen *Kontakt* mit einem lebenden Organismus voraussetzt, eine unvermittelt (akut) oder mit der Zeit (chronisch) auftretende Schädigungswirkung eines solchen in fester, flüssiger, gasförmiger oder plasmatischer Form vorliegenden Stoffes also erst dann bestehen kann, wenn ein Organismus diesem ausgesetzt (gewesen) ist und ihn in irgendeiner Weise (z. B. oral, dermal oder inhalativ) aufgenommen hat. So betrachtet sind auch Daten nicht *an sich* schädigend, sondern nur insofern, als sie gegenüber etwas oder jemandem eine entsprechende

Wirkung zeitigen.[7] Dies rechtfertigt den Vergleich von Daten mit einem Gefahrstoff wie beispielsweise Asbest (Véliz 2021: 107), chemisch an sich unbedenklichen faserförmigen Silikaten mit hervorragenden technischen Eigenschaften, die ihre Schädigungswirkung erst infolge einer Exposition gegenüber Asbestfasern entfalten können.

Kurzum: Was schädigend *wirkt*, muss nicht *an sich* schädigend *sein*. Dies gilt es auch bei der als toxikalisch bezeichneten Schädigungswirkung von Daten im Blick zu haben,[8] bei welcher zugleich, analog zur Toxizität als Schädigungswirkung eines Stoffes im biochemischen Kontext, zwischen einer quantitativen Komponente (Wirkstärke) und einer qualitativen Komponente (Wirkweise) unterschieden werden kann, was bei der nachfolgenden Konkretisierung von Datentoxikalität anhand ausgewählter Beispiele weiter zu bedenken sein wird.

## 2. Exemplarische Konkretisierungen

Angesichts der mannigfaltigen Mittel, Methoden und Möglichkeiten, Daten zu generieren, zu transferieren, zu analysieren und in irgendeiner Form nutzbar zu machen bzw. zu nutzen, haben wir es mit einem ebenso komplexen wie facettenreichen Phänomenbereich zu tun, dessen sachgemäße Erschließung eine multiperspektivische Betrachtungsweise erfordert, welche nicht nur differenziert genug ist, um Unterschiede zwischen einzelnen Phänomenen angemessen zu erfassen, sondern zugleich integriert genug, um ungerechtfertigte Trennungen zwischen ihnen zu vermeiden. Dies bedürfte einer wesentlich ausführlicheren systematischen Erörterung, wie sie im Rahmen dieses Beitrags nicht möglich ist. Im Folgenden kann es deshalb nur darum gehen, mit ständiger Rücksicht auf den spezifischen Unter-

---

7 Insofern kann gesagt werden: Daten sind weder gut noch schlecht, sondern indifferent (ἀδιάφορον). Sie befinden sich sozusagen in Möglichkeit (*in potentia*) gleichermaßen zum Guten wie zum Schlechten.

8 An dieser Stelle zeigt sich der Vorteil der Neubildung Datentoxikalität gegenüber der gleichermaßen denkbaren Rede von einer Toxizität von Daten (so z. B. Riedesel 2021: 412, der »data toxicity« allerdings versteht als »data that requires special handling«), welche die begriffliche Unschärfe in Kauf nehmen müsste, dass Gifte sowohl organische wie anorganische Stoffe sein können, während Toxine allein die von Lebewesen (einschließlich eukaryotischer Art) synthetisierten Gifte umfassen – ein Unterschied, der bei der Applikation des Toxizitätsbegriffs auf Daten sozusagen überschrieben wird.

suchungsgegenstand, für welchen ich zugleich mit Bedacht die zunächst eigens vorgestellte Begrifflichkeit verwende, ein paar strukturierende Breschen in dieses Dickicht zu schlagen.

In aller Vorläufigkeit kann hierzu zwischen Phänomenen unterschieden werden, in denen Daten – ungeachtet dessen, dass wir zumeist sagen, dass wir sie »nutzen« bzw. dass sie zur »Nutzung« existieren, was nahelegt, dass Daten gleichsam nur einen Nutzen haben – eine direkte Schädigungswirkung entfalten, und solchen mit indirekter Schädigungswirkung. Während bei ersteren eine Schädigung unmittelbar beabsichtigt und ganz bewusst angesteuert wird, erfolgt bei letzteren eine Schädigung mittelbar und wird sozusagen als Nebenwirkung in Kauf genommen. Während bei ersteren vornehmlich an Vorgänge zu denken ist, bei denen Daten von konkret identifizierbaren Subjekten gezielt zur Schädigung eines gleichermaßen konkret identifizierbaren Gegenübers eingesetzt werden und solche Schädigungen anzunehmenderweise auch leichter zum Vorschein kommen, handelt es sich bei Phänomenen indirekter Schädigungswirkung – jedenfalls wie sie hier im Blickpunkt stehen – um wesentlich schwieriger zu fassende Schädigungsvorgänge, die sich gegenüber einer breiteren Gemeinschaft oder der Öffentlichkeit überhaupt ereignen, ohne dass ein einzelner Urheber und eine direkte Verbindung zwischen Schädigendem und Geschädigtem identifizierbar ist.

Damit ist nicht bestritten, dass der so beschriebene Phänomenbereich wesentlich durch Übergängigkeit und Unabschließbarkeit charakterisiert ist und sich einzelne Phänomene zum Teil allenfalls schwerpunktmäßig einer der beiden Seiten zuordnen lassen. Ein Schubladendenken mit dem Anspruch, einzelne Phänomene in säuberlich getrennte Kategorien einzuordnen, ist auch an dieser Stelle fehl am Platz und demnach nicht der Anspruch der nachfolgenden orientierenden Bemerkungen.

## 2.1 Phänomene direkter Schädigungswirkung

Bei Phänomenen direkter Schädigungswirkung ist zunächst ganz allgemein an Situationen und Konstellationen zu denken, in denen personenbezogene, sicherheitsrelevante oder in irgendeiner Hinsicht sensible Daten – um einen in diesem Zusammenhang vielfach verwendeten somatischen Phraseologismus ebenfalls zu bemühen – »in falsche Hände« geraten (sind) und gezielt schädigend gegen andere Personen, Unternehmen oder Institutio-

nen eingesetzt werden. Diesen Formen des Datenmissbrauchs geht meist eine Variante des Datendiebstahls z. B. durch Phishing, Snarfing, Pharming oder Spoofing voraus[9], wobei die Motive durchaus unterschiedlich sein können, sei es primär pekuniär zur Löse- oder Schweigegelderpressung oder sei es primär um der Diskreditierung oder Desinformation eines Gegenübers willen, sodass vornehmlich dessen psychische oder soziale Schädigung bezweckt, eine gleichzeitige finanzielle Schädigung aber mehr oder weniger bewusst in Kauf genommen wird.

Persönliche Daten können durch andere aber auch gezielt als Waffe eingesetzt werden, wenn sie ohne Wissen der betreffenden Personen öffentlich gemacht werden, um diese bloßzustellen oder einzuschüchtern, wie es z. B. beim Doxxing der Fall ist (Douglas 2016: 199). Diese Form digitaler Gewalt wird vornehmlich gegen Prominente, Journalist*innen oder ehemalige Beziehungspartner*innen (zu Letzterem vgl. Bauer/Hartmann 2021: 76, 91), aber auch Vertreter*innen gegnerischer Positionen ausgeübt, was sowohl durch Einzelpersonen als auch durch Kollektive erfolgen kann. Letzteres etwa beim *Rénròu Sōusuǒ* (Chang/Leung 2015), einer vor allem in China und Taiwan verbreiteten Art virtuellem Lynchmob. Daten sind dann nicht nur in falschen Händen, sondern auch »am falschen Ort«.

Dieser Umstand, dass Daten eine schädigende Wirkung auch dadurch entfalten können, dass sie sich am falschen Ort befinden, macht solche deplatzierten Daten mit Schmutz vergleichbar – jedenfalls dann, wenn Schmutz im Anschluss an die britische Sozialanthropologin Mary Douglas allgemein und ohne Konnotation des Pathogenen und Unhygienischen definiert wird als »matter out of place« (1966: 36) – eine Sache nicht am Platz. Diese von Douglas wiederum dem britischen Diplomaten Philip Stanhope, 4. Earl of Chesterfield (1694–1773), zugeschriebene Schmutzdefinition (kritisch dazu Thompson 2021: 147 f.) setzt sowohl eine wie auch immer geartete Ordnung als auch zugleich einen Verstoß gegen dieselbe voraus, was Schmutz zu etwas Relativem macht. Schmutz ist demnach nie etwas Isoliertes, sondern steht immer in Beziehung zu einem ihn von sich ausschließenden System (Douglas 1966: 41). An einem Alltagsbeispiel verdeutlicht: »Essen ist nicht an sich schmutzig, aber es ist schmutzig, wenn

9 Für eine Übersicht vgl. Heartfield/Loukas 2018: 103 f. Als Spezialform von Datendiebstahl können Hackerattacken mittels datenlöschender Malware (Wiper) betrachtet werden, wie sie auch Teil der Kriegsführung – aktuell im Angriffskrieg Russlands gegen die Ukraine (Tidy 2022) – sein können.

man Kochutensilien im Schlafzimmer deponiert, oder Essen auf der Kleidung verschüttet« (ebd.: 36; meine Übersetzung, GS). Auf diesen bildlichen Vergleich von Daten mit Schmutz im angesprochenen Sinne, der freilich nicht überstrapaziert werden darf und doch die Ambivalenz von Daten auch im Blick auf ihre mögliche Schädigungswirkung gut zu veranschaulichen vermag, wird noch zurückzukommen sein.

Daten können toxikalisch schließlich auch dann sein, wenn sie manipuliert oder verfälscht werden – um im angesprochenen Bild zu bleiben: wenn man sie *ver*schmutzt. Charakteristisch für solches *data tampering* ist, dass Daten von anderen nicht einfach entwendet, sondern an Ort und Stelle belassen werden, und zwar gezielt verändert. Diese Veränderungen können ganz im Kleinen erfolgen, bis hin zur Modifizierung eines einzigen Pixels in einem Bild (Alberti u. a. 2019), was für die Betroffenen meist nur schwer ersichtlich ist, im Bereich etwa der Finanz- oder Betriebsbuchhaltung aber erheblichen Schaden verursachen kann. Selbst minimalinvasive Eingriffe in die Datenintegrität von Unternehmen können also von erheblicher wirtschaftlicher und damit zugleich sozialer Tragweite sein, was die von dem japanischen Ökonomen Hiroyuki Itami wirkmächtig vertretene Auffassung, die wertvollsten und für die Überlebensfähigkeit eines Unternehmens entscheidenden Vermögenswerte seien unsichtbar (Itami 1987: 12 f.), in einem anderen Licht erscheinen lässt. Die Erklärung von Daten – genauer: deren Monetarisierung,[10] Verwaltung und Erfassung – zum wichtigsten zukünftigen Vermögenswert von Unternehmen überhaupt, nicht nur, wie schon jetzt, im Bereich der Digitalwirtschaft, ist insofern dahingehend zu ergänzen, dass es sich hierbei zugleich um einen der gefährlichsten Vermögenswerte von Unternehmen handelt, der entsprechende Vorkehrungen und Schutzmaßnahmen unabdingbar macht. Die verschiedentlich, aber fälschlicherweise (Fanshawe 2022: 42 f.) dem US-amerikanischen Ökonom Peter F. Drucker zugeschriebene Managementweisheit »What gets measured gets managed« erweist sich in der heutigen Zeit von Big Data jedenfalls von ungeminderter, wenn nicht ungeahnter Aktualität.

Nicht weniger bedeutsam sowohl in wirtschaftlicher wie in sozialer Hinsicht ist die Sicherstellung und Sicherung der Datenintegrität im Bereich der kritischen Infrastruktur. Man denke, um ein Beispiel aus dem Sektor Transport und Verkehr anzuführen, an die bei einem zukünftigen digitalisierten Bahnbetrieb geplante Zug-zu-Zug-Kommunikation samt

10 Für einen Überblick vgl. Jentzsch 2019.

sensorbasierter Zuglokalisierung (Schomäcker 2019) oder, als Beispiel aus dem Gesundheitssektor, an die Arzneimittelherstellung (Schmitt 2019). Ganz grundsätzlich gilt dies auch für den Bereich der Wissenschaft, in dem schon kleinste, absichtliche oder unabsichtliche, Verfälschungen von Originaldaten und Datenbanken weitreichende Schädigungswirkungen auch im Sozialen entfalten können, wenn darauf z. B. die Verbreitung von Desinformation gründet oder sich daran anschließende gesellschaftliche Diskurse und politische Maßnahmen entsprechend kompromittiert sind. Das Streben nach höchstmöglicher Datenintegrität ist forschungspragmatischer Imperativ und, gemeinsam mit Datenqualität als einer die Verwendungsgerechtigkeit mit umschließenden Anforderung, geradezu *conditio sine qua non* für gute Wissenschaft, wobei eine Verletzung der Datenintegrität nicht nur bei fehlerhafter oder mangelnder Authentifizierung des Datenursprungs, sondern auch dann bestehen kann, wenn ambivalente, veraltete, redundante oder inkonsistente Datenbestände vorliegen (RfII 2019).

Die vorstehend dargestellten Phänomene direkter Schädigungswirkung durch entwendete, böswillig veröffentlichte oder in irgendeiner Hinsicht problembehaftete Daten machen deutlich, dass und inwiefern Daten toxikalisch nicht nur in Prozessen sozialer Interaktion, sondern auch auf der gesamtgesellschaftlichen Ebene wirken können. Wie die Oxforder Philosophin Carissa Véliz (2021: 107–139) anhand einschlägiger Beispiele aus Geschichte und Gegenwart darlegt, kann der falsche Umgang mit personenbezogenen Daten nicht nur die nationale Sicherheit eines Staates bedrohen (Stichwort: Equifax-Hack) oder zur Korrumpierung repräsentativ-demokratischer Regierungssysteme beitragen (Stichwort: Cambridge Analytica), sondern auch die gegenwärtige Sinn- und Orientierungskrise liberaler Gesellschaften noch weiter vorantreiben, etwa indem auf Social-Media-Plattformen eine Kultur narzisstischer Selbstdarstellung und selektiver Selbstjustiz befördert wird, was eine Korrektur des allgemeinen Umgangs mit personenbezogenen Daten unabdingbar macht. Dass vor dem Hintergrund der Auswirkungen einer zunehmend digitalisierten Lebenswelt überdies eine Re-Evaluation der bisherigen Vorstellung und Wahrnehmung von Privatsphäre und Öffentlichkeit in ihrem Verhältnis zueinander erforderlich ist, verdeutlichen auch die von Jürgen Habermas neuerlich angestellten Überlegungen »zu einem *erneuten* Strukturwandel der politischen Öffentlichkeit« (Habermas 2021: 470; meine Hervorhebung, GS) im Zuge

seiner ebenso bedenkenswerten wie nachdenklich stimmenden Revision der eigenen Theorie der politischen Öffentlichkeit.[11]

Mit letzteren Bemerkungen ist bereits der Übergang zur Reflexion darüber vollzogen, inwiefern Daten auch eine indirekte Schädigungswirkung entfalten können, die den bislang angesprochenen Phänomenen in ihrem Wirkpotenzial in nichts nachstehen müssen, auch wenn – oder vielleicht: gerade weil – die Schädigungswirkung prozesshaft schleichend, gleichsam hinter dem Rücken des Einzelnen und damit zunächst weniger augenfällig verlaufen mag.

## 2.2 Phänomene indirekter Schädigungswirkung

Ausgangspunkt für die im Vergleich zu Phänomenen direkter Schädigungswirkung ungleich schwieriger lokalisierbare und insofern potentiell weiterreichende, wenn auch in ihrer ganzen Tragweite noch nicht überschaubare indirekte Schädigungswirkung von Daten ist der Umstand, dass wir nicht lediglich durch gezielte Eingaben, sondern durch *jegliche* Internetaktivität und Nutzung digitaler Dienste permanent und unweigerlich Datenspuren hinterlassen (Wenhold 2018: 33–35).[12] Diese Datenspuren »zeichnen« gewissermaßen »ein digitales Abbild unseres Lebens« (Stampfl 2012: 394) und eröffnen Dritten nicht nur vielfältige, noch bis vor wenigen Jahren ungeahnte reale Möglichkeiten der Kontrolle und Bevormundung, aber auch der Gefahrenabwehr und Strafverfolgung, sondern können, durch gezielte Auswertung zu Nutzungs-, Kauf- und Bewegungsprofilen verdichtet, zugleich Aufschluss geben über Eigenschaften und Persönlichkeitsmerkmale eines Menschen einschließlich seiner sozialen Bezüge und Beziehungen.

---

11 So wie nicht alles Private auch politisch (hier im umfassenden aristotelischen Sinne als »die Polis betreffend«; πολιτικός von πολίς) sein muss, so muss nicht alles Private auch öffentlich sein – eine Aussage, die in der heutigen digital vernetzten Welt womöglich seltsam anmuten mag. Tatsächlich scheint Digitalität die Grenzlinie zwischen dem Privaten und dem Öffentlichen bei allem Haschen nach Likes und bei aller Gier nach Followern zunehmend zu verwischen.

12 Zur möglichen Unschärfe der Rede von Datenspuren vgl. Stäheli 2021: 66: »Die von den Verbindungen [der globalen Vernetzungsinfrastrukturen] produzierten Daten und Metadaten werden häufig als Datenspuren verstanden, wobei diese Metapher irreführend sein kann, da sie die arbiträre Beziehung zwischen dem Verbindungsgeschehen und den Daten übersieht. Die Akkumulation dieser Daten ist in der *corporate surveillance* zu einer der primären ökonomischen Kräfte geworden. Ihre Sammlung, Extraktion, Filterung, Prozessierung und Manipulation ermöglichen neue Formen der ökonomischen Wertschöpfung.«

Die Gesamtheit dieser z. B. beim Betreten der Online-Welt – jedenfalls ohne Proxy-Server oder Anonymisierungsnetzwerke – durch IP-Adresse, Cookies, Suchanfragen, Hardware- und Browsereinstellungen, Betriebssystem, installierte Software etc. generierten, individuell rückverfolgbaren Daten ist als »digitaler Fußabdruck« (Lambiotte u. a. 2014) eines Menschen nicht nur unverwechselbar, sondern auch gewissermaßen unhintergehbar: »Unlike footprints in the sand, digital traces in silica are not wiped away by the tide; instead, they accrete, leaving incredibly detailed records of social interaction« (Welser u. a. 2010: 117, Hervorhebung im Original weggelassen, GS). Das von Menschen in der Welt der Bits und Bytes bewusst oder unbewusst, absichtlich oder unabsichtlich hinterlassene Nebenprodukt der Datenspuren ist deshalb keineswegs wertloser Abfall,[13] sondern erweist sich für Dritte vielmehr als »Rohstoff« von unschätzbarem Wert, den es durch den Einsatz datenbasierter Technologien entsprechend abzubauen und ohne Rücksicht auf den ursprünglichen Kontext für neue Kontexte und Zwecke verwertbar zu machen gilt.[14] Selbst die augenscheinlich kostenlose Teilnahme am digitalen Leben kann sich damit als teuer erkauft erweisen – data non sunt gratis data.

Analog zu den beispielsweise mit der Gewinnung und Förderung mineralischer Rohstoffe einhergehenden unerwünschten Nebeneffekten für Mensch und Natur können negative realweltliche Folgen der Sammlung, Auswertung und Verarbeitung schier unendlicher Datenmengen beschrieben werden. Neben den enormen ökosozialen und sozioökonomischen Kosten der Digitalisierung und Datafizierung mitsamt ihrer globalen Ungleichverteilung (Parlamentarischer Beirat für nachhaltige Entwicklung des Deutschen Bundestages 2019: 2) ist auf die schädlichen Umwelteinwirkungen hinzuweisen, die direkt oder indirekt auf datengetriebene

13 Wenn überhaupt und mit Blick speziell auf den Schädigungsaspekt könnten Datenspuren als eine Art »Sondermüll« ganz eigener, nämlich *digitaler* Art bezeichnet werden, der dem Recycling zur Wieder- und Neuverwendung zugeführt wird, wohingegen unter »dark data« oder »zombie data« primär »unutilized or underutilized data« zu verstehen sind – »typically data that was collected and used for a single purpose, then forgotten about and often archived« (Laney 2018: 42).

14 Zu diesem Prozess und den verschiedenen metaphorischen Sprechweisen im Sinne des Data-Mining vgl. van Dijck 2014: 198–201; Thylstrup 2019: 2 f. Kritisch zum Bild von Daten als Rohstoff und dessen Abbau – zumindest, wenn damit ein allgemeingültiger »Mechanismus der Rekontextualisierung und Verarbeitung von Daten« suggeriert und die Aufwertung von »Daten zu faktisch Vorfindlichem« (Püschel 2014: 17) praktiziert werde, vgl. Püschel 2014: 10 u. 14 ff. Speziell zu den Prozessen der De- und Rekontextualisierung von Daten speziell für den Gesundheitsbereich vgl. Deutscher Ethikrat 2018: 14 f., 47 f. und 86–88.

Infrastrukturen zurückgehen (Bietti/Vatanparast 2020). Es wird geschätzt, dass die Informations- und Kommunikationstechnologiebranche bis zum Jahr 2040 – ohne entsprechende Gegenmaßnahmen – für über 14 % der globalen Treibhausgasemissionen (bei Zugrundelegung der Zahlen von 2016) verantwortlich sein wird (Belkhir/Elmeligi 2018), während aktuellen Berechnungen zufolge der Anteil allein der Rechenzentren (»Server-Farmen«) am weltweiten Stromverbrauch von 1,15 % im Jahr 2016 auf knapp 2 % im Jahr 2030 steigen wird und dieser Anstieg auch durch etwaige Effizienzgewinne aufgrund von technologischen Innovationen nicht gänzlich aufgefangen werden kann (Koot/Wijnjoven 2021: 7 f. u. 11). Um ein Beispiel zu nennen: Die Rechenzentren in der selbsternannten Internet-Hauptstadt Europas Frankfurt am Main verbrauchen mittlerweile deutlich mehr Strom als der Frankfurter Flughafen und sind, wie Zahlen aus dem Jahr 2018 zeigen, für rund ein Fünftel des Gesamtstromverbrauchs der Stadt Frankfurt verantwortlich (Wacket 2020); die enorme, bislang ungenutzte Abwärme der Rechenzentren soll in verschiedenen Pilotprojekten für das Heizen von Büro- und Wohngebäuden nutzbar gemacht werden (Rittel 2021), gewissermaßen »Heizen mit Datenverkehr« (Janović 2021). Die Rede von schädlichen Daten ist also mehrdeutiger als es zunächst scheint.

Auch digitale Datenspuren selbst sind, wie die dänische Kommunikationswissenschaftlerin Nanna Bonde Thylstrup argumentiert, nicht adiaphorisch, als aus ethischer Sicht neutrale Phänomene, sondern insofern als »Schadstoff« zu betrachten, als sie der ökonomischen Logik der Extraktion folgten, während sie zugleich durch die Spuren der Körper gekennzeichnet blieben, von denen sie ursprünglich stammten (Thylstrup 2019: 2 und 4). Überhaupt gründe, so die Autorin, die Logik der Datafizierung »on a logic of waste and recycling, with significant implications for how we consider datafication's politics and ethics« (Thylstrup 2019: 1). Wie Thylstrup unter Rekurs auf Sarah Myers West weiter ausführt, etabliere die Kommerzialisierung von Daten[15] eine Logik des Datenkapitalismus, welche der Macht der Netzwerke dadurch den Vorrang einräume, dass sie quer zur wirtschaftlichen, politischen und sozialen Dimension der Technologie aus den in den Netzwerken generierten Datenspuren Werte schaffe (Thylstrup 2019: 2; dazu West 2019: 21). Darin zeige sich eine deutliche Affinität zum Konzept des Überwachungskapitalismus (*surveillance capitalism*) von Shoshana

15 Zu Chancen und Risiken datenbasierter bzw. datengetriebener Geschäftsmodelle vgl. Kretschmer 2018: 459–462.

Zuboff, die darunter eine neue »Unterart des Kapitalismus« versteht, »bei dem die Gewinne aus der einseitigen Überwachung und Veränderung menschlichen Verhaltens stammen« (Zuboff 2016; dazu Myers West 2019: 23). Diese datenkapitalistische Wertschöpfungskette, aber auch die von datenintensiven Unternehmen zuweilen bewusst durch die Überproduktion von Daten gleichermaßen produzierte wie reproduzierte »organisatorische Ignoranz« (Schwarzkopf 2020: 197) gilt es im Blick zu behalten, wenn Daten als strategische Gegenwartsressource (»das neue Öl«; vgl. Spitz 2017: 9) und Datenökosysteme[16] als »Betriebssysteme der zukünftigen globalen datengetriebenen Wirtschaft« (Fraunhofer-Verbund IUK-Technologie [2021]) betrachtet werden.

Die mit der digitalen Transformation aller Lebensbereiche (»Vierte industrielle Revolution«) einhergehende Datafizierung unseres Daseins[17] mit entsprechenden Folgen auch für unser Verständnis desselben erweist sich spätestens dann aber als selbstgestellte Falle, wenn die *scheinbare* digitale Freiheit, ob bewusst oder nicht, um den Preis *realer* Unfreiheit erkauft wird und Menschen dadurch, dass ihnen die Möglichkeit digitaler Selbstbestimmung[18] verwehrt wird, an der Ausschöpfung potenzieller individueller

16 Für eine aktuelle Definition von »Datenökosystem« auf fachliterarischer Basis vgl. Putnings 2021: 7: »Ein Datenökosystem ist das prägende, ganzheitliche Umfeld, in dem verschiedene Akteure zusammenkommen, um Daten zu produzieren, anzubieten, zu finden und zu »konsumieren« (d.h. nachzunutzen, zu verarbeiten, anzureichern, zu archivieren, zu publizieren, Entscheidungen darauf zu fällen etc.). Die Einflüsse des Datenökosystems wirken in alle Phasen der Datenlebenszyklen hinein, es schafft die entsprechenden *Rahmen-, Netzwerk- und regulativen Bedingungen* für die (Zusammen-)Arbeit mit Daten bzw. stellt diese konkret dar.«

17 Digitalisierung (»Umwandlung analoger Informationen in ein maschinenlesbares Format« [Mayer-Schönberger/Cukier 2017: 106) und Datafizierung (»Umwandlung von allem nur Vorstellbaren […] in Datenform, um sie damit quantifizieren zu können« [Mayer-Schönberger/Cukier 2017: 24]) sind dahingehend zu differenzieren, dass Digitalisierung zwar als »Turbolader der Datafizierung«, nicht aber als »Ersatz dafür« (ebd.) fungiert. Zur immer weiter fortschreitenden Digitalisierung unseres Alltags, einschließlich der zunehmenden Verlagerung wesentlicher Aspekte der Persönlichkeit ins Digitale, und der Datafizierung des Sozialen vgl. Filipović 2015: 7 ff. und die Beiträge bei Houben/Prietl 2018.

18 Zum Begriff der »digitalen Selbstbestimmung« vgl. Mertz u. a. 2016: 18, die darunter – im Rückgriff auf die Definition »allgemeiner« Selbstbestimmung durch den Deutschen Ethikrat (2013: 120 f.) – »[d]ie konkrete Entfaltung einer menschlichen Persönlichkeit bzw. die Möglichkeit der Realisierung von je eigenen Handlungsentwürfen und Handlungsentscheidungen« verstehen, »soweit dies eine bewusste Verwendung digitaler Medien betrifft oder dies von der Existenz oder Funktionsweise digitaler Medien (mit-)abhängig ist«, und insgesamt sieben Begriffskomponenten identifizieren: Kompetenz, Informiertheit, Werte, Freiwilligkeit, Wahlmöglichkeit, Willensbildung und Handlung (Mertz u. a. 2016: 21–26).

Entfaltungs- und Verwirklichungsmöglichkeiten wirksam gehindert werden. Auf diese Aktualisierungsbedürftigkeit des Konzepts der strukturellen Gewalt[19] unter digitalen Vorzeichen und die aufgrund umfassender digitaler Vernetzung heute nicht mehr nur als Orwell'sche Dystopie, sondern als allzu reale Gefahr erscheinende ubiquitäre und omnipräsente Überwachung von Menschen »bis in die Tiefe der Gefühls- und Gedankenwelt« (Lobo 2014) hinein – kurz: auf die Gefahr einer ›digitalen Diktatur‹ (Aust/Ammann 2014: 7 ff.)[20], deren Vorboten keineswegs allein in autoritären Regimen, sondern auch in Staaten der »Freien Welt« (Stichwort: Gläserne Belegschaft[21]) sichtbar sind, sei an dieser Stelle wenigstens hingewiesen.

Mit all dem soll keinem ostentativen Fortschrittsskeptizismus das Wort geredet, geschweige denn unter Zuhilfenahme düsterer Weltuntergangsmetaphorik die Unausweichlichkeit derselben beschworen, wohl aber die realistische Einsicht in die alles durchstimmende Ambivalenz menschlicher Lebenswirklichkeit ausgesprochen werden, wonach sich durch den rasanten Fortschritt im Bereich der Informations- und Kommunikationstechnologien nicht nur neue Möglichkeiten und Wege eines lebensdienlichen Gebrauchs dieser Technologien, sondern zugleich immer auch neue Möglichkeiten und Wege auftun, sie zur Verfolgung, Unterdrückung und Schädigung anderer zu missbrauchen. Doch allein in Form skeptischer Negation scheinen technikethische Bemerkungen wenig zielführend. Daher sollen im abschließenden Abschnitt in aller Kürze noch einige kritisch-konstruktive Überlegungen aus technikethischer Perspektive dazu angestellt werden, wie einer Schädigungswirkung von Daten begegnet werden könnte.

---

19 Zur Unterscheidung zwischen personaler und struktureller Gewalt vgl. Galtung 1971: 9 ff.; dazu Schreiber 2022: 80–92. Es sei bemerkt, dass die Identifizierung von Gewalt*verhältnissen* bereits lange Zeit vor Galtung erfolgt ist, z. B. bei Marx 1962 [1867]: 765 u. 790.

20 Vgl. dazu Stefan Aust in einem Interview von 2014: »Diese totale Kontrolle, der der Mensch sich teils freiwillig, teils unfreiwillig unterwirft, ist, wenn Sie so wollen, eine Art von Diktatur. Und ich glaube, es ist wahrscheinlich die strengste Diktatur, was die Überwachung anbetrifft, die es jemals auf dieser Erde gegeben hat« (zitiert nach Baetz 2014: Abs. 2).

21 Vgl. dazu die umfangreiche Studie von Christl 2021.

## 3. Vergessenwerden durch Unauffindbarmachen

Wie im biochemischen Kontext die Toxizität von Stoffen nicht einfach eliminiert, aber der Umgang mit toxischen Stoffen entsprechend gestaltet und, wann immer notwendig, angepasst werden kann, so ist angesichts des vorstehend beleuchteten Phänomens der Datentoxikalität zu fragen, wie einer Schädigungswirkung von Daten im Bereich menschlichen Zusammenlebens begegnet werden kann. Dies zum Anlass zu nehmen, um über die Sinnhaftigkeit dessen zu räsonieren, dass überhaupt Daten in gegebenem, weitreichenden Umfang mittels digitaler Techniken gesammelt und gespeichert werden, wäre freilich müßig, zumal ein generelles Verbot des Sammelns und Speicherns beispielsweise speziell von personenbezogenen Daten[22] – von Fragen der politischen Durchsetzbarkeit und praktischen Umsetzbarkeit desselben einmal abgesehen – mit allem potentiell oder tatsächlich Schädlichen zugleich auch das potentiell oder tatsächlich Förderliche dieser Praxis beseitigen würde.[23] Nicht das Sammeln und Speichern von Daten als solches, sondern die Art und Weise, *wie* Daten aller Arten und Komplexitätsgrade gesammelt und gespeichert werden und zukünftig gesammelt und gespeichert werden sollten, steht zur Diskussion. Hierbei rückt – nicht nur, aber nicht zuletzt – im Falle personenbezogener Daten Fragen der Ver- und Entschlüsselung, der Zugangs- und Zugriffskontrolle, aber auch der Löschung und Löschbarkeit in den Fokus.

Es ist an dieser Stelle nicht der Ort, das aus dem Recht auf informationelle Selbstbestimmung[24] folgende »Recht auf Vergessenwerden«, wie es in

---

22 Hierauf scheinen mir die Überlegungen z. B. bei Véliz 2021: 108 u. 112 hinauszulaufen, die im Sammeln und Speichern personenbezogener Daten »a ticking bomb, a disaster waiting to happen« (108) sieht. Und weiter: »Personal data is dangerous because it is sensitive, highly susceptible to misuse, hard to keep safe, and desired by many – from criminals to insurance companies and intelligence agencies. The longer our data is stored, and the more it is analysed, the more likely it is that it will end up being used against us. Data is vulnerable, which in turn makes data subjects and anyone who stores it vulnerable too« (108). Nicht unähnlich Schneier 2019: 212 f.

23 Ebenso wenig lösungsorientiert (jedenfalls aus gesamtgesellschaftlicher Perspektive) wäre daher eine gemeinschaftliche Suche nach dem Heil in der Flucht in eine digitale Wüste, gewissermaßen ein Eremitentum »2.0«, aber auch pauschale Forderungen nach einer »Entdatafizierung«. Reflexionen über »Taktiken der Entnetzung« (Zurstiege 2019) und Fragen der Verantwortlichkeit des Einzelnen als Daten-Prosumer sind gleichwohl keineswegs obsolet.

24 Zur Herleitung des Rechts auf informationelle Selbstbestimmung (im Sinne eines Datenschutz-Grundrechts) aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG vgl. BVerfG 1983. Kritisch dazu z. B. Assion 2014.

Art. 17 der neuen EU-Datenschutz-Grundverordnung (DSGVO) verbrieft ist, en détail zu erörtern.[25] Dies soll nur insofern geschehen, als damit die Frage der Löschung und Löschbarkeit von Daten tangiert ist. Die Möglichkeit und Sicherstellung der Löschung und Löschbarkeit von Daten erweist sich nämlich als Schlüssel, wenn auch nicht als Allheilmittel, um insbesondere Phänomenen direkter Schädigungswirkung von Daten, wie sie aus deren Diebstahl, böswilliger Veröffentlichung oder Verfälschung resultieren können, entgegenzuwirken und bereits eingetretene Schädigungswirkungen abzumindern. Dabei ist einerseits zu bedenken, wie eine solche Löschung zu verstehen ist – in der DSGVO wird der Begriff »Löschen« nicht näher definiert.[26] Und andererseits muss gefragt werden, wie die dann so oder so verstandene Löschung auch im Falle toxikalischer Daten umgesetzt werden kann.

Was zunächst das *Verständnis* betrifft, ist entscheidend, dass das vielerorts in der öffentlichen Diskussion, zuweilen auch im juristischen Kontext missverständlich verkürzend[27] als »Recht auf Vergessen« bezeichnete »Recht auf Vergessenwerden« einen *aktiven* und *selektiven* Prozess zum Gegenstand hat. Dieser entspricht dem gleichermaßen aktiven und selektiven Prozess der Erinnerung (ανάμνησις), im Unterschied zum passiven Gedächtnis (μνήμη) – wenn auch eben im Modus der Verkehrung. Im Unterschied zur alltagssprachlichen Rede von Vergessen, aber auch der alltagsweltlichen Erfahrung von Erinnern und Vergessen[28] meint Vergessen*werden* in diesem Zusammenhang also etwas anderes als dass etwas *von selbst*, durch einen natürlichen Vorgang bzw. mit der Zeit, aus dem Gedächtnis verloren geht und so allmählich in Vergessenheit gerät. Vielmehr beschreibt Vergessen-

---

25 Für eine solche vgl. Luch u. a. 2014; Abbt 2016a und b.

26 Interessanterweise wird in den Begriffsbestimmungen von Art. 4 DSGVO »Löschen« als eine Variante der »Verarbeitung« von Daten betrachtet, wobei »Löschen« (*erasure*) und »Vernichtung« (*destruction*) mit der Konjunktion »oder« einander nebengeordnet (»[…] die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung«) werden, was – selbst wenn das »oder« als einschließendes (lateinisch *vel*) und nicht als ausschließendes (lateinisch *aut*) »oder« gemeint sein sollte – einen semantischen Unterschied zwischen Löschen und Vernichtung markiert.

27 Selbst von seinem Begriffsschöpfer, dem österreichischen Rechtswissenschaftler Viktor Mayer-Schönberger (Mayer-Schönberger 2012), sowie vom Bundesverfassungsgericht (BVerfG 2019a; 2019b). Zum Hintergrund vgl. ferner Hunzinger 2018: 34–38.

28 Pointiert z. B. Jahnel/Pallwein-Prettner 2022: 111 (unter Rekurs auf Mayer-Schönberger): »Für unser Gehirn [ist] das Erinnern die Ausnahme und das Vergessen die Regel. Für ein digitales Gerät ist es aber genau umgekehrt, hier erfordert das Vergessen einen aktiven Akt, das Erinnern geschieht automatisch.«

werden das Ergebnis eines intentional geleiteten und methodisch angeleiteten Löschungs*vorgangs*. Gleich ob Löschung dabei im strengen Sinne als Auslöschung (Eliminierung) oder im weiten Sinne als Beseitigung oder Entfernung verstanden wird – das Recht auf Vergessenwerden bezeichnet das Recht auf die unverzügliche Durchführung von Löschungsvorgängen[29], die im Falle personenbezogener Daten *zugleich* die »Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten« (Art. 17 Abs. 2 DSGVO) beinhaltet. Löschung von Daten im Sinne des Rechts auf Vergessenwerden bedeutet demnach nicht einfach nur »Erschwerung des Zugriffs auf Daten« (Abbt 2016a: 353; vgl. Abbt 2016b: 927), sondern Löschung von Daten *sowohl* »am Ort ihrer ersten Speicherung und Veröffentlichung« *als auch* an allen anderen Stellen, an denen die betreffenden Daten »veröffentlicht, archiviert oder verlinkt worden sind« (Buchner 2020: 307). Es geht mit einem Wort darum, diese Daten, einschließlich möglicher Datenrückstände in Archivspeichern, »aus der (Online-)Welt zu schaffen« (Herbst 2020: Rn. 49; zitiert bei Buchner 2020: 307).

Nun ist allerdings, und dies betrifft die *Umsetzung* solcher Löschungsvorgänge, nicht zu Unrecht die Frage aufgeworfen worden, ob das Löschen von Daten in einem Informationszeitalter wie dem unseren, in dem Menschen ständig und allerorten von einer Flut von Informationen überschüttet werden[30] und das, wie angesprochen, vom rasanten Fortschritt im Bereich der Informations- und Kommunikationstechnologien nachhaltig geprägt, wenn nicht gar getrieben ist, überhaupt »noch eine Zukunft« habe und nicht vielmehr als »Utopie der Moderne« (Hunzinger 2018: 213; vgl. 240)

29 Dass derartige Löschungsvorgänge auch vor dem Hintergrund des in Abschnitt 2.1. angestellten Vergleichs toxikalischer Daten mit Schmutz sowie der in Abschnitt 2.2 angesprochenen Grundlegung der Logik der Datafizierung in einer Logik von Abfall und Recycling bei Thylstrup beschrieben werden können – letzteres insofern, als Recycling selbst ein »Prozess zur Abfallvernichtung« durch Transformation von Abfall und Wiederzuführung durch Neubewertung, mithin ein Löschungsprozess ist, nämlich der »Zukunft des Dings als eben dieses Ding sowie dessen Vergangenheit« (Gehrlein 2020: 110) –, ist nur offensichtlich. Ebenso der radikale Widerspruch zum Vergessenwerden der Namen und Werke von Menschen nach ihrem Tod, wie es z. B. in der altägyptischen, klassisch-griechischen, aber auch biblischen Tradition gerade als »Unglück« gilt: »Der, der sein Vergessen beklagt, fühlt sich bereits wie ein Toter« (120; vgl. 119–122). Zu entsprechenden Lösungsansätzen für einen »digitalen Nachlass« vgl. Brucker-Kley 2013: 82–84.

30 Zur informationstechnischen Aufladung der Umgebung des Menschen wie überhaupt der »informatorische[n] Aufladung der physischen Welt« durch eine allgegenwärtige IKT vgl. Grunwald 2010: 85 f.

zu betrachten sei. In der Tat scheint eine endgültige und vollständige Löschung von Daten samt aller Datenrückstände zumindest im Internet in seiner heutigen Form, aber auch in Systemen der Künstlichen Intelligenz (KI), die von einer gleichermaßen komplexen Verarbeitung wie einer schnellen und unabsehbaren Verbreitung von Daten gekennzeichnet sind (Jorzig/Sarangi 2020: 138), nahezu unmöglich. Selbst wenn das Recht auf Vergessenwerden als »Menschenrecht« (Gstrein 2016) oder »Internet-Grundrecht« (Boehme-Neßler 2014) *geltend gemacht* werden kann, ist damit also noch nichts darüber gesagt, wie einem solchen Recht auch *Geltung verschafft* werden kann, wird doch in der Diskussion über das Recht auf Vergessenwerden geradezu gebetsmühlenartig betont, dass das Internet nichts vergesse.[31] Das sprichwörtliche Steckerziehen oder eine einfache, sichere Vernichtung von Daten wie durch die physische Zerstörung als Unbrauchbarmachung eines Speichermediums ist hier gerade nicht möglich und widerspricht überdies der »Logik digitaler Archive« (Stähli 2021: 416), zumal Löschungsvorgänge selbst wiederum Spuren erzeugen können, die dann ebenfalls zu beseitigen wären, woraus sich theoretisch ein infiniter Regress ergäbe.

So berechtigt die Forderung nach einem Recht auf Vergessenwerden ist, so illusorisch erscheint die Vorstellung einer einfachen praktischen Umsetzung desselben. Dies gilt umso mehr im Falle toxikalischer Daten, die als solche ja nicht nur in der Online-Welt, sondern auch in der Offline-Welt Spuren hinterlassen haben[32], sodass es nicht lediglich um ihre Löschung, sondern zugleich um ihre möglichst effektive realweltliche »Unschädlichmachung« gehen müsste. Was jedenfalls die Online-Welt betrifft, scheint mir ein theoretisch gangbarer Weg in der Rekonzeptualisierung des traditionellen Löschungsbegriffs zu liegen. Angesichts des oben bereits angesprochenen Umstandes, dass wir in der Online-Welt sozusagen auf Schritt und Tritt rückverfolgbare Datenspuren hinterlassen, kann es bei dem allgemein als Löschung bezeichneten Vorgang im Grunde nur darum gehen, ebendiese Rückverfolgbarkeit an einer bestimmten, und zwar der (jeweils) richtigen, Stelle zu un-

31 Zu diesem »Ewigkeitseffekt« vgl. Stumpf 2017: 40–44.

32 In der Offline-Welt allerdings kann »Vergessen« gerade der *falsche* Weg sein, selbst wenn er als »Therapeutikum« betrachtet werden sollte, wird doch das Trauma einer Vergangenheit nicht durch Vergessen bewältigt, sondern gerade durch »Erinnern, um zu überwinden« (Assmann 2020: 202). Zu dieser ethischen Verpflichtung zum Erinnern als Vergegenwärtigung der Vergangenheit und Chance kritischer Selbstreflexion, bei der Vergessen *kein* angemessenes therapeutisches Mittel ist, vgl. Assmann 2020: 180–202, hier bes. 191 ff.

terbrechen, um damit eine Wiederauffindbarkeit auszuschließen.[33] Es geht dann also »nicht mehr um das (letztlich unmögliche) physische Auslöschen von Datenspuren, sondern um die Nichtlokalisierbarkeit von Daten« (Stähli 2021: 416). Kurzum: Das Recht auf Vergessenwerden wird – zumindest in den Fällen, in denen eine dauerhafte und irreversible »Entfernung« von Daten nicht möglich ist – nicht durch Löschung qua »Tilgung« von Daten, sondern durch deren *Unauffindbarmachung* umgesetzt.[34]

Wie der Schweizer Soziologe Urs Stäheli in seiner Studie *Soziologie der Entnetzung* (2021) darlegt, lässt sich das Konzept der »Unauffindbarkeit« (*irretrievability*) von Daten, verstanden als »dritte Kategorie zwischen Speichern und Löschen« (417), bis auf Ideen zu einer »›Kompostierung‹ überflüssiger Daten« in den 1990er Jahren zurückverfolgen. An die Stelle eines auf Konservierung ausgerichteten Digitalarchivs, dessen größtes *Risiko* in der Unauffindbarkeit von Daten besteht, ist eine solche in einer Sammlung »entnetzte[r] Daten« gewissermaßen Programm: »einzelne Elemente wie etwa Links oder Formulare bleiben funktionsfähig, sind nun aber herausgerissen aus jedem intelligiblen Zusammenhang. Der Datenabfall kann so gesammelt, aber nicht mehr durchsucht werden.« (Ebd.) Angesichts der angedeuteten Schwierigkeiten der Umsetzung und Sicherstellung einer Löschung von Daten scheint das Konzept der Unauffindbarkeit und damit eine Realisierung des Vergessenwerdens durch Unauffindbarmachen nicht nur bedenkenswert, sondern auch intuitiv nachvollziehbar. Dies sei abschließend an einem Beispiel erläutert.

Am Ende des Films *Raiders of the Lost Ark* (deutscher Filmtitel: *Jäger des verlorenen Schatzes*) von Steven Spielberg und George Lucas, dem ersten Teil der Abenteuerfilmreihe *Indiana Jones* aus dem Jahr 1981, fragt Universitätskurator Brody in einer Besprechung mit amerikanischen Regierungsvertretern, wo sich denn jener von Dr. Jones vor den Händen der Nazis für die ameri-

---

33 Derartige Ansätze zu anonymen Kommunikationsverfahren gibt es in der Informatik bereits seit Anfang der 1980er Jahre, vgl. Schwenke 2006: 245–249.

34 »Entfernung« und »Tilgung« in Anführungszeichen, um dem Umstand Rechnung zu tragen, dass ein konventioneller Löschungsvorgang technisch gesehen *nicht* die Entfernung (im Sinne von Wegschaffung) von Daten, sondern lediglich deren Markierung als gelöscht zur Folge hat, was allenfalls bloß deren Wiederauffindbarkeit erschwert. Beim konventionellen Löschen werden also nur »die Verweise auf die Daten im Index, dem Inhaltsverzeichnis der Festplatte, gelöscht und der Bereich zum Überschreiben freigegeben. Dieses Überschreiben findet aber möglicherweise nie statt. Die vermeintlich entsorgten Daten befinden sich auch weiterhin auf der Festplatte, sind aber für den Nutzer nicht mehr mit normalen Mitteln erreichbar« (Bundesamt für Sicherheit in der Informationstechnik o. J.).

kanische Regierung gerettete »verlorene Schatz« – nichts Geringeres als die alttestamentliche Bundeslade, einer aus Akazienholz verfertigten, mit Gold überzogenen Truhe – nun befinde, worauf er von Major Eaton zur Antwort erhält, dass sich die Lade »an einem sehr sicheren Ort« befinde (»The Ark is somewhere very safe«), um von Topspezialisten untersucht werden zu können. In der Schlussszene sieht man dann, wie ein Lagerarbeiter die Lade in eine einfache Holzkiste samt Aufschrift »Top Secret Army Intel 9906753 Do Not Open!« verstaut, welche daraufhin, mit einem simplen Vorhängeschloss gesichert, in ein schier unendlich großes Lager gebracht wird und in der Masse tausender und abertausender ähnlich aussehender Holzkisten untergeht.

Eine Erörterung der vielfältigen Deutungen, die dieses Filmende erfahren hat, kann an dieser Stelle unterbleiben. Ich beschränke mich auf eine von Rainer Erlinger (2019: 127–132) vorgeschlagene Deutung, die – auf unseren Zusammenhang übertragen – zugleich eine anschauliche Antwort auf die Frage liefert, wie das Unauffindbarmachen auch toxikalischer Daten verstanden werden könnte. In der Tat befindet sich die Bundeslade, die ja nicht nur von unschätzbarem Wert, sondern auch von ungeahnter Macht und Kraft im Guten wie im Schlechten ist, »an einem sehr sicheren Ort«, indem sie zwischen unzählig vielen ähnlich aussehenden Dingen versteckt ist, was einen Versuch, sie zu finden, als praktisch aussichtslos erscheinen lässt. Das sicherste Versteck eines Gegenstandes ist nicht unbedingt ein bestimmter Ort (klischeehaft: der Dachboden oder der Keller), sondern ein ganz und gar *un*bestimmter Ort. Was Erlinger in Bezug auf das Bild mit den unzähligen Holzkisten in der Schlussszene des Films *kritisch* über die Unterdrückung von Wahrheit sagt, die heutzutage eben nicht mehr nur durch Zensur oder Gewalt, sondern durch ein Untergehen inmitten anderer Informationen erfolgen könne, kann im *positiven* Sinne als Veranschaulichung der Entnetzung von Daten zum Zwecke ihrer Unauffindbarmachung verstanden werden:

> »Es reicht, so viele andere Kisten zu produzieren, dass man kaum mehr eine Chance hat, die eine Kiste, in der sich die Wahrheit befindet, zu finden oder, wenn man sie gefunden hat, sicher zu identifizieren. Die Wahrheit ist nur eine Information unter vielen, die sich von den anderen lediglich dadurch unterscheidet, dass sie der Realität entspricht. Das lässt sich aber der Kiste von außen nicht unbedingt ansehen.« (Erlinger 2019: 128 f.)

Inwieweit nun ein solches theoretisches Konzept des »Ablegens in einen falschen Ordner« zur Unauffindbarmachung von Daten praktisch realisiert

werden kann, um damit Phänomenen der Datentoxikalität zu begegnen, steht freilich auf einer anderen Seite.

# Literatur

Abbt, Christine (2016a): Ich vergesse. Über Möglichkeiten und Grenzen des Denkens aus philosophischer Perspektive. Frankfurt am Main: Campus.

Abbt, Christine (2016b): Recht auf Vergessen? Ethik der zweiten Chance? Überlegungen zum Urteil des Europäischen Gerichtshofes (EuGH) vom 13.5.2014. In: Deutsche Zeitschrift für Philosophie 64(6), 925–946.

Abromeit, Heidrun (1999): Volkssouveränität in komplexen Gesellschaften. In: Brunkhorst, Hauke/Niesen, Peter (Hg.): Das Recht der Republik. Frankfurt am Main: Suhrkamp, 17–36.

ACCC (2019): Digital platforms inquiry – final report, 16. July 2019. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [30.3.2022].

Acemoglu, Daron/Makhdoumi, Ali/Malekian, Azarakhsh/Ozdaglar, Asuman (2020): Too Much Data: Prices and Inefficiencies in Data Markets. https://economics.harvard.edu/files/economics/files/acemoglu_spring_2020.pdf [30.3.2022].

Acquisti, Alessandro/Brandimarte, Laura/Loewenstein, George (2020): Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. In: Journal of Consumer Psychology 30(4), 736–758.

Acquisti, Alessandro/Grossklags, Jens (2005): Privacy and Rationality in Individual Decision Making. In: IEEE Security and Privacy 3(1), 26–33.

Akerlof, George A. (1970): The Market for »Lemons«: Quality Uncertainty and the Market Mechanism. In: The Quarterly Journal of Economics 84(3), 488–500.

Alberti, Michele u.a. (2018): Are You Tampering with My Data? In: Proceedings of the European Conference on Computer Vision (ECCV) Workshops. https://arxiv.org/abs/1808.06809 [28.02.2022].

Amlinger, Carolin (2021): Schreiben. Eine Soziologie literarischer Arbeit, Berlin: Suhrkamp.

Appenzeller, Arno/Bretthauer, Sebastian/Birnstill, Pascal (2021): Datensouveränität für Patienten im Gesundheitswesen. In: Datenschutz und Datensicherheit (DuD), 173–179.

Arendt, Hannah (1994): Freiheit und Politik. In: Zwischen Vergangenheit und Zukunft. Übungen im politischen Denken I. München/Zürich: Piper, 201–226.

Arendt, Hannah (2002): Vita activa oder vom tätigen Leben. München/Zürich: Piper.

Arendt, Hannah (2003): Was ist Politik? München/Zürich: Piper.

Arendt, Hannah (2007): The Great Tradition: I. Law and Power. In: Social Research 74(3), 713–726.

Arendt, Hannah (2011a): Über die Revolution, München/Zürich: Piper.

Arendt, Hannah (2011b): Eichmann in Jerusalem. Ein Bericht von der Banalität des Bösen, München/Zürich: Piper.

Arendt, Hannah (2012): Das Urteilen, München/Zürich: Piper.

Arning, Marian Alexander/Rothkegel, Tobias (2022). In: Taeger, Jürgen/Gabel, Detlev (Hg.): DSGVO BDSG TTDSG. München: Beck 2022.

Artikel-29-Datenschutzgruppe (2013): Stellungnahme 03/2013 zur Zweckbindung (WP 203), angenommen am 02.04.2013.

Art. 29 WP [= Article 29 Data Protection Working Party] (2014): Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [10.3.22]
= Artikel-29-Datenschutzgruppe (2014): Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, angenommen am 09.04 2014.

Assmann, Aleida (2013, ³2020): Das neue Unbehagen an der Erinnerungskultur. Eine Intervention. München: Beck.

Augsberg, Ino (⁷2015): GRC Art. 7 Achtung des Privat- und Familienlebens. In: von der Groeben, Hans/Schwarze, Jürgen/Hatje, Armin (Hg.): Europäisches Unionsrecht. Baden-Baden: Nomos, Rn. 1–13.

Augsberg, Steffen (2013): Die Innovationsoffenheit des Rechts und die Gestaltungsaufgabe der Rechtswissenschaft – dargestellt am Beispiel innovativer Versorgungsstrukturen im Gesundheitswesen, Jahrbuch des öffentlichen Rechts 61, 579–597.

Augsberg, Steffen/von Ulmenstein, Ulrich (2018): Modifizierte Einwilligungserfordernisse: Kann das Datenschutzrecht vom Gesundheitsrecht lernen? In: GesundheitsRecht, 341–347.

Aust, Stefan/Ammann, Thomas (2014): Digitale Diktatur. Totalüberwachung, Datenmissbrauch, Cyberkrieg. Düsseldorf/Berlin: Econ.

Baetz, Brigitte (2014): Datenspuren im Netz. Überwachung in der »digitalen Diktatur«. In: Deutschlandfunk, 27.10.2014. https://www.deutschlandfunk.de/datenspuren-im-netz-ueberwachung-in-der-digitalen-diktatur-100.html [28.02.2022].

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace (Davos, 8.2.1996). Electronic Frontier Foundation 1996. https://www.eff.org/cyberspace-independence [5.2.2022].

Basedow, Jürgen (2019): Vorbemerkung (zu § 305) u. §§ 305 ff. In: Oetker, Harmut/Rixecker, Roland/Säcker, Franz Jürgen/Limperg, Bettina (Hg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 2. München: Beck.

Bauer, Jenny-Kerstin/Hartmann, Ans (2021): Formen digitaler geschlechtsspezifischer Gewalt. In: bff/Bundesverband Frauenberatungsstellen und Frauennotrufe, Nivedita Prasad (Hg.): Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung. Formen und Interventionsstrategien. Bielefeld: transcript, 63–99.

BDI [= Bundesverband der Deutschen Industrie] (2021): Mit »GAIA-X« in Richtung einer europäischen Datensouveränität. https://bdi.eu/artikel/news/mit-gaia-x-in-richtung-einer-europaeischen-datensouveraenitaet/ [09.3.2022].

Beck, Ulrich (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp.

Becker, Maximilian (2021): Consent Management Platforms und Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung — Real Time Bidding auf Basis von Nutzerprofilen als Ausprägung der Personendatenwirtschaft. In: Computer und Recht (CR) 17, 87–98.

Beise, Clara (2021): Datensouveränität und Datentreuhand. In: Recht digital (Rdi) 2, 597–599.

Beise, Clara/Eckes, Tim (2021): ZEVEDI-Tagung: Datensouveränität. Probleme und Gestaltungschancen. In: Multimedia und Recht (MMR) 24 »Aktuell«, Nr. 444186. https://rsw.beck.de/cms/?toc=mmr.130&docid=444187 [25.02.2022].

Belkhir, Lotfi/Elmeligi, Ahmed (2018): Assessing ICT global emissions footprint. Trends to 2040 & recommendations. In: Journal of Cleaner Production 177, 448–463.

Belko, Simone (2021): Digitale Mündigkeit. Wie das Internet die Demokratie retten kann. In: Researchgate [Belko]. https://doi.org/10.13140/RG.2.2.15112.75527 [13.1.2022]

Benrath, Bastian/Löhr, Julia (2021): Europäisches Cloud-Projekt. Wie Gaia-X dafür sorgt, dass man trockenen Fußes zur Arbeit kommt. In: FAZ vom 15.10.2021. https://www.faz.net/aktuell/wirtschaft/digitec/wie-gaia-x-dafuer-sorgt-dass-man-trockenen-fusses-zur-arbeit-kommt-17587199.html [15.3.2022].

Benz, Arthur ([2]2010): Governance – Regieren in Komplexen Regelsystemen: Eine Einführung. Wiesbaden: VS Verlag für Sozialwissenschaften.

Benz, Arthur/Lütz, Susanne/Schimank, Uwe/Simonis, Georg (Hg.) (2007): Handbuch Governance. Theoretische Grundlagen und empirische Anwendungsfelder. Wiesbaden: Springer VS.

Berg, Sebastian/Rakowski, Niklas/Thiel, Thorsten (2020): Die digitale Konstellation. Eine Positionsbestimmung. In: Zeitschrift für Politikwissenschaft 30, 171–191.

Berlin, Isaiah (1969): Two concepts of liberty. In: Four essays on liberty. Oxford: Oxford University Press, 118–172.

bidt [= Bayerisches Forschungsinstitut für Digitale Transformation] (o. J. [2022]): Datensouveränität [Glossar]. https://www.bidt.digital/glossar-datensouveraenitaet/ [15.3.2022].

Bietti, Elettra/Vatanparast, Roxana (2020): Data Waste. In: Harvard International Law Journal Frontiers 61, 1–11. https://harvardilj.org/2020/04/data-waste [28.02.2022].

Bilsky, Leora Y. (2008): Citizenship as Mask: Between the Imposter and the Refugee. In: Constellations 15(1), 72–97.

Bilsky, Leora Y. (2009): »Speaking through the Mask«: Israeli Arabs and the Changing Faces of Israeli Citizenship. In: Middle East Law and Governance 1, 166–209.

Bizer, Johann (1999): Der Datentreuhänder. Lösungsmodell für den Datenzugang der Forschung. In: Datenschutz und Datensicherheit, 392–395.

Blankertz, Aline (2020): Designing Data Trusts. Why We Need to Test Data Trusts Now. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf [25.3.2022].

BMBF [= Bundesministerium für Bildung und Forschung] (2020): Natürlich. Digital. Nachhaltig. Ein Aktionsplan des BMBF. Berlin: Bundesdruckerei.

BMWi [= Bundesministerium für Wirtschaft und Energie] (2016): Digitale Strategie 2025. Stand März 2016. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.pdf?__blob=publicationFile&v=18 [5.2.2022].

BMWi (2019): Das Projekt Gaia-X. Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems. Stand Oktober 2019. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=24 [15.3.2022].

BMWi (2020a): A franco german Position on Gaia-X. https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10 [15.3.2022].

BMWi (2020b): GAIA-X. Technical Architecture. Stand Juni 2020. https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=7 [15.3.2020].

BMWi (2020c): Gaia-X: Für ein digital souveränes Europa. Deutschland, Frankreich und weitere Partner verfolgen das Ziel einer europäischen vertrauenswürdigen Dateninfrastruktur. In: Schlaglichter der Wirtschaftspolitik 9. https://www.bmwi.de/Redaktion/DE/Publikationen/Schlaglichter-der-Wirtschaftspolitik/schlaglichter-der-wirtschaftspolitik-09-2020.pdf?__blob=publicationFile&v=40 [15.3.2022].

BMWi (2020d): GAIA-X: Driver of digital innovation in Europe. Featuring the next generation of data infrastructure. Stand Mai 2020. https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8 [15.3.2022].

BMWK [= Bundesministerium für Wirtschaft und Klimaschutz] (2022): Der deutsche Gaia-X Hub. https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html [15.3.2022].

Bodin, Jean (1976): Über den Staat, herausgegeben von Gottfried Niedhart. Stuttgart: Reclam.

Boehme-Neßler, Volker (2014): Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht. In: Neue Zeitschrift für Verwaltungsrecht (NZW) 33(13), 825–830.

Böhme, Gernot (1993): Am Ende des Baconschen Zeitalters. Frankfurt am Main: Suhrkamp.

Böhme, Gernot (2008): Ethik leiblicher Existenz. Frankfurt am Main: Suhrkamp.

Böschen, Stefan/Schneider, Michael/Lerf, Anton (Hg.) (2004): Handeln trotz Nichtwissen. Frankfurt am Main: Campus.

Botta, Jonas (2021): Delegierte Selbstbestimmung? PIMS als Chance und Risiko für einen effektiven Datenschutz. In: Multimedia und Recht (MMR) 24, 946–951.

Britz, Gabriele (2005): Freie Entfaltung durch Selbstdarstellung. Tübingen: Mohr Siebeck.

Britz, Gabriele (2010): Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In: Hoffmann-Riem, Wolfgang (Hg.): Offene Rechtswissenschaft, Tübingen: Mohr Siebeck, 561–596.

Brucker-Kley, Elke u.a. (2013): Sterben und Erben in der digitalen Welt. Von der Tabuisierung zur Sensibilisierung. Zürich: Vdf.

Brunhöber, Beatrice (2011): Souveränität. Herkunft und Zukunft eines Schlüsselbegriffs von Dieter Grimm. In: Der Staat 50, 123–126.

Brunkhorst, Hauke (1999): Hannah Arendt. München: Beck.

Buchner, Benedikt (2020): Art. 4 Nr. 11. In: Kühling, Jürgen/Buchner, Benedikt (Hg.): DS-GVO BDSG. München [3]2020.

Buchner, Benedikt (2020): Grundsätze des Datenschutzrechts. In: Tinnefeld, Marie-Theres u.a.: Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. Berlin/Boston: De Gruyter Oldenbourg [7]2020, 220–332.

Budras, Corinna (2021): Sorge um Datensouveränität: »Bundescloud« wegen Microsoft-Beteiligung in der Kritik. https://www.faz.net/aktuell/wirtschaft/cloud-fuer-behoerden-wegen-microsoft-beteiligung-in-der-kritik-17569277.html [29.3.2022].

Bundesamt für Sicherheit in der Informationstechnik (o.J.): Daten auf Festplatten und Smartphones endgültig löschen. https://t1p.de/91qw7 [28.02.2022].

Bundeskartellamt (2019): Beschluss B6-22/16 vom 6. Februar 2019. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html [25.3.2022].

Bundesrat (2021): Europäische Datensouveränität schützen. Berlin. https://www.bundesrat.de/SharedDocs/drucksachen/2021/0301-0400/340-21.pdf?__blob=publicationFile&v=1 [16.3.2022].

Bundesregierung (o. J. [2020]): Digitalgipfel in Dortmund: Datensouveränität ist höchstes Gebot. https://www.bundesregierung.de/breg-de/themen/digitalisierung/kanzlerin-bei-digitalgipfel-1686406 [29.3.2022].

Bundesregierung (2021a): Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Kabinettfassung, 27. Januar 2021. https://www.bundesregierung.de/resource/blob/992814/1845634/45aee6da9554115398cc6a722aba08cb/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1 [5.2.2022].

Bundesregierung (2021b): Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien. https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-zur-regelung-des-datenschutzes-und-des-schutzes-der-privatssphaere-in-der-telekommunikation-und-bei-telemedien.pdf?__blob=publicationFile&v=6 [9.3.2022].

Bunnenberg, Jan Niklas (2020a): Privatautonomie und Datenschutz. In: JuristenZeitung 75, 1088–1097.

Bunnenberg, Jan Niklas (2020b): Privates Datenschutzrecht. Baden-Baden: Nomos.

Busche, Jan (2021): Vorbemerkung (zu § 145). In: Oetker, Harmut/Rixecker, Roland/Säcker, Franz Jürgen/ Limperg, Bettina (Hg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 1. München: Beck.

Bydlinski, Franz (1967): Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts. Wien: Springer.

Bydlinski, Franz (1996): System und Prinzipien des Privatrechts. Wien: Springer.

Caffarra, Cristina/Scott Morton, Fiona (2021): The European Commission Digital Markets Act: A translation. Vox.eu. https://voxeu.org/article/european-commission-digital-markets-act-translation [25.3.2022].

Canovan, Margaret (1983): Arendt, Rousseau, and Human Plurality in Politics. In: The Journal of Politics 45(2), 286–302.

Celikates, Robin (2017): »Veränderungen an sich sind immer das Ergebnis von Handlungen außerrechtlicher Natur«. Subjektive Rechte, ziviler Ungehorsam und Demokratie nach Arendt. In: Rechtsphilosophie. Zeitschrift für Grundlagen des Rechts (RphZ) 3(1), 31–43.

Chang, Lennon/Leung, Andy (2015): An introduction of cyber-crowdsourcing (human flesh searching) in the Greater China region. In: Smith, Russell G. u. a. (Hg.): Cybercrime Risks and Responses. Eastern and Western Perspectives. New York: Palgrave, 240–252.

Choi, Jay Pil/Jeon, Doh-Shin/Kim, Byung-Cheol (2019): Privacy and personal data collection with information externalities. In: Journal of Public Economics 173, 113–124.

Christl, Wolfie (2021): Digitale Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management? Eine Studie von Cracked Labs. Wien, September 2021. https://crackedlabs.org/daten-arbeitsplatz [28.02.2022].

CMA [= Competition & Markets Authority] (2020): Online platforms and digital advertising – Market study final report. July 2020. https://assets.publishing.service.gov.uk/media/5efc57ed3a6 f4023d242ed56/Final_report_1_July_2020_.pdf [25.3.2022].

Cohen, Jean L. (2007): Sovereignty and Rights: Thinking with and beyond Hannah Arendt. In: Heinrich-Böll-Stiftung (Hg.): Hannah Arendt: Verborgene Tradition – Unzeitgemäße Aktualität? Berlin: Akademie, 291–310.

Couture, Stephane/Toupin, Sophie (2019): What does the notion of »sovereignty« mean when referring to the digital? In: New Media & Society 21, 2305–2322.

Crouch, Colin (2008): Postdemokratie. Frankfurt am Main: Suhrkamp.

Datenethikkommission (2019): Gutachten der Datenethikkommission der Bundesregierung (23.10.2019). https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 [9.3.2022]. Inzwischen auch in: Spiecker gen. Döhmann, Indra/Bretthauer, Sebastian (Hg.), Dokumentation zum Datenschutz mit Informationsfreiheitsrecht, Loseblatt. Baden-Baden: Nomos (Stand: 84. Ergänzungslieferung 2021).

Datenschutzkonferenz (2017a): Grundsatzpositionen und Forderungen für die neue Legislaturperiode. https://www.datenschutz-bayern.de/dsbk-ent/GRUND_01-DSK.html [5.2.2022 – das Dokument wird auf der Webseite der DSK selbst nicht mehr vorgehalten].

Datenschutzkonferenz (2017b): Göttinger Erklärung: Vom Wert des Datenschutzes in der digitalen Gesellschaft. https://www.datenschutzkonferenz-online.de/media/en/20170330_en_goettinger_erklaerung.pdf [5.2.2022].

Datenschutzkonferenz (2019): Hambacher Erklärung zur Künstlichen Intelligenz. Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 03.04.2019. https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf [25.3.2022].

Datenschutzkonferenz (2021): Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021. https://datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf [30.3.2022].

de Streel, Alexandre/Feasey, Richard/Krämer, Jan/Monti, Giorgio (2021): Making the Digital Markets Act more resilient and effective. CERRE Recommendations Paper, May 2021. https://dx.doi.org/10.2139/ssrn.3853991 [25.3.2022].

DellaVigna, Stefano (2009): Psychology and Economics: Evidence from the Field. In: Journal of Economic Literature 47(2), 315–372.

Der Bayerische Landesbeauftragte für den Datenschutz (2021): Orientierungshilfe, Bayerische öffentliche Stellen und Telemedien Erläuterungen zum neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). www.datenschutz-bayern.de/datenschutzreform2018/OH_TTDSG_Telemedien.pdf [15.3.2022].

Deutscher Ethikrat (2013): Die Zukunft der genetischen Diagnostik – von der Forschung in die klinische Anwendung. Stellungnahme. Berlin: Ethikrat. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-zukunft-der-genetischen-diagnostik.pdf [30.3.2022].

Deutscher Ethikrat (2018): Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme (2017). Berlin: Ethikrat. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf [9.3.2022].

Di Fabio, Udo (2020): GG Art. 2. In: Maunz/Dürig (Hg.): Grundgesetz-Kommentar Bd. I. München: Beck, Rn. 1–91.

Die Landesbeauftragte für den Datenschutz Niedersachsen (2021): Stellungnahme zum TTDSG im Rahmen der Länderbeteiligung, vom 22.01.2021. https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-TTDSG/landesbeauftragte-datenschutz-niedersachsen.pdf?__blob=publicationFile&v=4 [25.3.2022].

Dietmar Jahnel/Angelika Pallwein-Prettner ($^{3}$2021): Datenschutzrecht. Wien: Facultas.

Digital Gipfel (2019): Digitale Souveränität im Kontext plattformbasierter Ökosysteme. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3 [15.3.2022].

Digital Gipfel (2020): Digitale Souveränität und Resilienz: Voraussetzungen, Treiber und Maßnahmen für mehr Nachhaltigkeit Digital-Gipfel-Plattform 2 »Innovative Digitalisierung der Wirtschaft«, Fokusgruppe Digitale Souveränität. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/digitale-souveraenitaet-und-resilienz.pdf?__blob=publicationFile&v=10 [15.3.2015].

Digital Regulation Project (2021): Consumer Protection for Online Markets and Large Digital Platforms. Policy Discussion Paper No. 1 (May 20. 2021). https://tobin.yale.edu/sites/default/files/pdfs/digital%20regulation%20papers/Digital%20Regulation%20Project%20-%20Consumer%20Protection%20-%20Discussion%20Paper%20No%201.pdf [25.3.2022].

Dijck, José van (2014): Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society 12(2), 197–208.

Douglas, David M. (2016): Doxing: A Conceptual Analysis. In: Ethics and Information Technology 18(3), 199–210.

Douglas, Mary (1966): Purity and Danger. An Analysis of Concepts of Pollution and Taboo. London: Routledge 2000.

Dreier, Horst (2013): GG Art. 2 I. In: Ders. (Hg.): Grundgesetz Kommentar, 1. Präambel, Artikel 1–19, Bd. 1. Tübingen: Mohr Siebeck [3]2013, Rn. 1–99.

Drexl, Josef (1998): Die wirtschaftliche Selbstbestimmung des Verbrauchers. Tübingen: Mohr Siebeck.

Duden ([6]2020): Das Herkunftswörterbuch. Etymologie der deutschen Sprache. Berlin: Bibliographisches Institut.

Eberl, Oliver/Niesen, Peter (2011): Immanuel Kant: Zum ewigen Frieden. Kommentar. Berlin: Suhrkamp.

Eberl, Oliver/Salomon, David (2017): Perspektiven sozialer Demokratie in der Postdemokratie. Wiesbaden: Springer VS.

Eckes, Tim (2011): Personelle Gewaltenteilungslehre und parlamentarische Demokratie. In: Eberl, Oliver (Hg.): Transnationalisierung der Volkssouveränität. Radikale Demokratie diesseits und jenseits des Staates. Stuttgart: Steiner.

Efroni, Zohar/Metzger, Jakob/Mischau, Lena/Schirmbeck, Marie (2019): Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. In: European Data Protection Law Review (EDPL) 5(3), 352–366.

EMGR [= Europäischer Gerichtshof für Menschenrechte] (1997): Z v. Finland. Urt. v. 25.2.1997 – Az. 22009/93.

EGMR (2004): von Hannover v. Germany. Urt. v. 24.6.2004 – Az. 59320/00.

EGMR (2010): Schüth v. Germany. Urt. v. 23.09.2010 – Az. 1620/03.

EGMR (2018): FNASS v. France. Urt. v. 18.01.2018 – Az. 48151/11 u. 77769/13.

Eifert, Martin (2015): Das Allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 GG. In Juristische Ausbildung (Jura) 2015, 1181–1191.

EPRS [= European Parliament] (2021): Ideas Paper. Towards a more resilient EU: Digital sovereignty for Europe. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf [5.2.2022].

Erlinger, Rainer (2019): Warum die Wahrheit sagen? Frankfurt am Main: Fischer.

Ernst, Stefan (2017): Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO, Zeitschrift für Datenschutz (ZD) 8, 110–114.

Ernst, Stefan (2020): Die Widerruflichkeit der datenschutzrechtlichen Einwilligung. In: Zeitschrift für Datenschutz (ZD) 11, 383–385.

Etrillard, Stéphane (2006): Prinzip Souveränität. Ihre Konstante in einer komplexen Welt – als souveräner Persönlichkeit sicher entscheiden und handeln. Paderborn: Junfemann.

EuGH (2010): Urt. v. 09.11.2020 – Az. C-92, 93/09.

Europäische Datenschutzausschuss (2018): Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der ePrivacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation, angenommen am 25. Mai 2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_de.pdf [30.3.2022].

Europäische Datenschutzausschuss (2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 Version 1.1, angenommen am 04.05.2020. edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf [9.3.2022].

Europäische Kommission (2020a): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie. https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_de.pdf [20.02.2022].

= Europäische Kommission (2020a): Communication: A European Strategy for Data. COM(2020) 66 final.

Europäische Kommission (2020b): Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz), Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0767&from=DE [11.03.2022]. = Europäische Kommission (2020b): Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). COM(2020) 767 final.

Europäische Kommission (2020c): Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). COM(2020) 842 final.

Europäische Kommission (2022a): Kommission schlägt Maßnahmen für eine faire und innovative Datenwirtschaft vor. Pressemitteilung vom 23.2.2022. https://ec.europa.eu/commission/presscorner/api/files/document/print/de/ip_22_1113/IP_22_1113_DE.pdf [15.3.2022].

Europäische Kommission (2022b): Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM(2022) 68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN [30.3.2022].

Europäischer Datenschutzausschuss (2020): Erklärung zur ePrivacy-Verordnung und zur künftigen Rolle der Aufsichtsbehörden und des EDSA, angenommen am 19. November 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_de.pdf [25.3.2022].

Europäischer Rat (2020): Erklärung v. 02.10.2020, EUCO 13/20, Nr. 9 (5). https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf [9.3.2022].

Europäischer Rat (2021a): Erklärung v. 25.03.2021, SN 18/21, Nr. 6 lit. c (4). https://www.consilium.europa.eu/media/49005/250321-vtc-euco-statement-de.pdf [9.3.2022].

Europäischer Rat (2021): Regulation on Privacy and Electronic Communications. Erwägungsgrund 20 lit. aa im Dokument Nr. 6087/21 (S. 24) vom 10.02.2021. https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf [9.3.2022].

Europäischer Datenschutzbeauftragter (2020): Personal Information Management Systems. In: TechDispatch 2/2020. https://edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf [25.3.2022].

Europäisches Parlament (2017): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017PC0010&from=DE [25.3.2022].

Europäisches Parlament (2020): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance, 25.11.2020. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0767&from=EN [25.3.2022].

Europäisches Parlament (2021): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM/2021/206 final, Brüssel, den 21.4.2021. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=DE [25.3.2022].

Europäisches Parlament (2022): Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23.03.2022, https://ec.europa.eu/newsroom/dae/redirection/document/83521 [9.3.2022].

Europäisches Parlament und Rat der EU (2016): Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. In: Amtsblatt der Europäischen Union L 119, 4. Mai 2016, 1–88. http://data.europa.eu/eli/reg/2016/679/oj [28.02.2022].

European Data Protection Supervisor (2016): EDPS Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data, Opinion 9/2016. https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf [30.3.2022].

Fanshawe, Simon (2022): The Power of Difference. Where the Complexities of Diversity and Inclusion Meet Practical Solutions. London, New York: Kogan Page.

FAZ (2020): EU-Kommission: Amazon spielt gegen die Regeln. In: FAZ vom 10.11.2020. https://www.faz.net/aktuell/wirtschaft/digitec/eu-kommission-wirft-amazon-missbrauch-seiner-plattform-vor-17045563.html#void [15.3.2022].

Fetter, Frank (1905): The Principles of Economics with Applications to Practical Problems. New York: The Century Co.

Fezer, Karl-Heinz (2017): Data Ownership of the People. An Intrinsic Intellectual Property Law Sui Generis Regarding People's Behaviour-genereated Informational Data. In: Zeitschrift für geistiges Eigentum (ZGE) 9, 356–370.

Fezer, Karl-Heinz (2017a): Dateneigentum der Bürger, Zeitschrift für Datenschutz (ZD) 8, 99–105.

Fezer, Karl-Heinz (2017b): Dateneigentum. In: Multimedia und Recht (MMR) 20, 3–5.

Fezer, Karl-Heinz (2019): Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft. In: Schriftenreihe Stiftung Datenschutz, Dateneigentum und Datenhandel Bd. 3. Berlin: Erich Schmidt, 101–160.

Filipović, Alexander (2015): Die Datafizierung der Welt. Eine ethische Vermessung des digitalen Wandels. In: Communicatio Socialis 48(1), 6–15.

Fischer, Joseph (2019): Im Konflikt zwischen USA und China ist Europa auf verlorenem Posten. Vor allem technologisch gerät Europa im Konflikt zwischen USA und China unter Druck. Die Herausforderung ist die Verteidigung der Datensouveränität. https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-im-konflikt-zwischen-usa-und-china-ist-europa-auf-verlorenem-posten/24888988.html [14.3.2022].

Floridi, Luciano (2020): The Fight for Digital Sovereignty: What It Is, and Why it Matters, Especially for the EU. In: Philosophy & Technology 33, 369–378. https://doi.org/10.1007/s13347-020-00423-6 [5.2.2022].

Flume, Werner ([4]1992): Allgemeiner Teil des Bürgerlichen Rechts. Berlin: Springer.

Fokusgruppe Datenschutz (2020): Datenmanagement- und Datentreuhandsysteme. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020, Version 1.0. 2020. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf [9.3.2022].

Forbrukerrådet (2018): Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy. https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design [25.3.2022].

Forst, Rainer (2007): Republikanismus der Furcht und der Rettung. Zur Aktualität der politischen Theorie Hannah Arendts. In: Heinrich-Böll-Stiftung (Hg.): Hannah Arendt: Verborgene Tradition – Unzeitgemäße Aktualität? Berlin: Akademie, 229–240.

Fossen, Thomas (2015): Judgment and imagination in Habermas' theory of law. In: Philosophy & Social Criticism 41(10), 1069–1091.

Foucault, Michel (2004): Geschichte der Gouvernementalität I. Sicherheit, Territorium, Bevölkerung. Frankfurt am Main: Suhrkamp.

Fraser, Lindley M. (1939): The Doctrine of Consumers' Sovereignty. In: Economic Journal 49(195), 544–548.

Fraunhofer-Verbund IUK-Technologie (o.J. [2021]): Themen: Datenökosysteme. https://www.iuk.fraunhofer.de/de/themen/datenoekosysteme.html [28.02.2022].

Friedrichsen, Mike/Bisa, Peter-J. (2016): Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft. Wiesbaden: Springer VS.

Fritsch, Michael ([10]2018): Marktversagen und Wirtschaftspolitik – Mikroökonomische Grundlagen staatlichen Handelns. München: Franz Vahlen.

Fröhlich, Ernst (1992): Vom zwingenden und nichtzwingenden Privatrecht. Aarau: Sauerländer.

Gabriel, Sigmar (2015): Rede von Bundesminister Gabriel auf der Konferenz zur digitalen Transformation in Kreativwirtschaft, Handel und Mobilität. https://www.bmwi.de/Redaktion/DE/Reden/2015/20150918-rede-gabriel-konferenz-digitaler-wandel.html [15.3.2022].

Gabriel, Sigmar (2016): Nationaler IT-Gipfel 2016: Eröffnungsrede. BMWK, 17.11.2016. https://www.de.digital/DIGITAL/Redaktion/DE/IT-Gipfel/Video/2016/rede-sigmar-gabriel.html [15.3.2021].

Gaia-X AISBL [= Gaia-X European Association for Data and Cloud AISBL] (2021a): Visions & Strategy. Stand Dezember 2021. https://gaia-x.eu/sites/default/files/2021-12/Vision%20%26%20Strategy.pdf [15.3.2022].

Gaia-X AISBL (2021b): Gaia-X Architecture Document. Stand Dezember 2021 https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf [15.3.2022].

Gaia-X AISBL (2021c): Gaia-X Policy Rules Document. Stand November 2021. https://gaia-x.eu/sites/default/files/2022-01/Policy_Rules_Document_21.11.pdf [15.3.2022].

Gaia-X AISBL (2021d): Gaia-X Labelling Framework. https://gaia-x.eu/sites/default/files/2021-11/Gaia-X%20Labelling%20Framework_0.pdf [15.3.2022].

Gaia-X AISBL (2021e): Gaia-X Federation Services (GXFS). Stand Dezember 2021. https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Federation_Services_White_Paper_1_December_2021.pdf [15.3.2022].

Gaia-X AISBL (2021 f): Glossary. https://www.gaia-x.eu/glossary [14.3.2022].

Gaia-X AISBL (2021 g): Standards. https://www.gaia-x.eu/what-is-gaia-x/standards [14.3.2022].

Galtung, Johan (1971): Gewalt, Frieden und Friedensforschung. In: Galtung, Johan: Strukturelle Gewalt. Beiträge zur Friedens- und Konfliktforschung. Reinbek bei Hamburg: Rowohlt 1975, 7–36.

Gehring, Petra (2021): Statement Datensouveränität. In: Gesammelte-Statements_PGr-DS_11052021 [Unpubliziertes Arbeitsmanuskript der ZEVEDI-Projektgruppe »Datensouveränität«], 2–3.

Gehrlein, Christina (2020): Abfallverbindungen. Verworfenes und Verwerfungen in Erzähltexten der deutschsprachigen Gegenwartsliteratur. Bielefeld: transcript.

Gennermann, Paula (2020): Call for Papers 2020. https://www.gwmt.de/wp-content/uploads/CfP_Toxikalita%CC%88t_2020_Erfurt.pdf [28.02.2022].

Gerhardt, Volker (1996): Vom Willen zur Macht. Anthropologie und Metaphysik der Macht am exemplarischen Fall Friedrich Nietzsches. Berlin/New York: De Gruyter.

Gethmann, Carl Friedrich/Buxmann, Peter/Diestelrath, Julia/Humm, Bernhard G./Lingner, Stephan/Nitsch, Verena/Schmidt, Jan C./Spiecker, gen. Döhmann, Indra (2022):

Künstliche Intelligenz in der Forschung. Neue Möglichkeiten und Herausforderungen für die Wissenschaft. Heidelberg/New York: Springer.

Golland, Alexander (2021): Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien BT-Drucksache 19/27441, 03.05.2021. https://www.bundestag.de/resource/blob/836010/498ffdbeff45200bdc011b13acc38b31/19-9-1054_Stellungnahme_SV_Dr_Golland_PwC_Legal_oeA_TTDSG_21-04-2021-data.pdf [9.3.2022].

Golland, Alexander/Riechert, Anne (2022). In: Riechert, Anne/Wilmer, Thomas (Hg.): Berliner Kommentar zum TTDSG, Berlin 2022 [Im Erscheinen].

Gounot, Emmanuel (1912): L'autonomie de la volonté en droit privé. Paris: Rousseau.

Graef, Inge/Clifford, Damian/Valcke, Peggy (2018): Fairness and enforcement: Bridging competition, data protection, and competition law. In: International Data Privacy Law 8(3), 200–223.

Graef, Inge/Van Berlo, Sean (2021): Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility. In: European Journal of Risk Regulation 12(3), 674–698.

Grimm, Dieter (2009): Souveränität Herkunft und Zukunft eines Schlüsselbegriffs. Berlin: Berlin University Press.

Große Kracht, Hermann-Josef (2021): »Solidarität zuerst!« Zur Neuentdeckung einer politischen Idee, Bielefeld: transcript.

Grunwald, Armin (2002): Technikfolgenabschätzung – zur Einführung. Berlin: Sigma.

Grunwald, Armin (2010): Virtualisierung von Kommunikation und Handeln im Pervasive Computing – Schritte zur Technisierung des Menschen? In: Bölker, Michael/Gutmann, Mathias/Hesse, Wolfgang (Hg.): Information und Menschenbild. Berlin/Heidelberg: Springer, 78–101.

Gstrein, Oskar Josef (2016): Das Recht auf Vergessenwerden als Menschenrecht – Hat Menschenwürde im Informationszeitalter Zukunft? Baden-Baden: Nomos.

Gutmann, Thomas (2001): Freiwilligkeit als Rechtsbegriff. München: Beck.

Habermas, Jürgen (1992, $^{5}$1995): Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt am Main: Suhrkamp.

Habermas, Jürgen (1995): Theorie des kommunikativen Handelns. Frankfurt am Main: Suhrkamp.

Habermas, Jürgen (1998): Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt am Main: Suhrkamp.

Habermas, Jürgen (2021): Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit. In: Seeliger, Martin/Sevignani, Sebastian (Hg.): Ein neuer Strukturwandel der Öffentlichkeit? Baden-Baden: Nomos, 470–500.

Hacke, Jens (2006): Philosophie der Bürgerlichkeit. Die liberalkonservative Begründung der Bundesrepublik. Göttingen: Vandenhoek & Ruprecht.

Hacker, Philipp (2019): Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht. In: Zeitschrift für die gesamte Privatrechtswissenschaft 4, 148–197.

Haltern, Ulrich (2007): Was bedeutet Souveränität? Tübingen: Mohr Siebeck.

Hanloser, Stefan (2021): Schutz der Geräteintegrität durch § 25 TTDSG. In: Zeitschrift für Datenschutz (ZD) 12, 399–403.

Hansen, Marit (2021): Datenschutz und Datensouveränität. Vortragsfolien. https://www.datenschutzzentrum.de/uploads/vortraege/20211011_DatenschutzDatensouveraenitaet_ZEVEDI_Hansen.pdf [5.2.2022].

Hartl, Andreas/Ludin, Anna (2021): Recht der Datenzugänge. Was die Datenstrategien der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen. In: Multimedia und Recht (MMR) 24, 534–538.

Hartung, Johanna ([2]2006): Sozialpsychologie. Stuttgart: Kohlhammer.

Hayek, Friedrich A. von (1968): Wettbewerb als Entdeckungsverfahren. Kiel: Universität, Institut für Weltwirtschaft.

Heartfield, Ryan/Loukas, George (2018): Protection Against Semantic Social Engineering Attacks, in: Conti, Mauro/Somani, Gaurav/Poovendran, Radha (Hg.): Versatile Cybersecurity. Cham: Springer Nature, 99–140.

Hefeker, Carsten (2020): Europas Industrie- und Handelspolitik: Eine Bewertung der deutschen und europäischen Strategien aus ökonomischer Sicht. In: Zeitschrift für Europarechtliche Studien (ZEuS) 23(2), 227–238.

Heinelt, Hubert (Hg.) (2018): Handbook on Participatory Governance. Cheltenham: Edward Elgar.

Herbst, Tobias (2020): Art. 17 Recht auf Löschung (»Recht auf Vergessenwerden«). In: Kühling, Jürgen/Buchner, Benedikt: Datenschutz-Grundverordnung BDSG. Kommentar. München [3]2020: Beck, 499–527.

Hippelainen, Leo/Oliver, Ian/Lal, Shankar (2017): Towards Dependably Detecting Geolocation of Cloud Servers. In: Yan, Zheng/Molva, Refik/Mazurczyk, Wojciech/Kantola, Raimo (Hg.): Network and system security. Cham: Springer Nature, 643–656.

Hoeren, Thomas (2013): Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht. In: Multimedia und Recht (MMR) 16, 486–491.

Hoeren, Thomas (2019): Datenbesitz statt Dateneigentum. In: Multimedia und Recht (MMR) 22, 5–8.

Hoffmann-Riem, Wolfgang (1998): Informationelle Selbstbestimmung in der Informationsgesellschaft. In: Archiv des öffentlichen Rechts (AöR) 123, 514–540.

Hofmann, Jeanette (2019): Mediatisierte Demokratie in Zeiten der Digitalisierung: Eine Forschungsperspektive. In: Hofmann, Jeanette/Kersting, Norbert/Ritzi, Claudia/Schünemann, Wolf J. (Hg.): Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven. Bielefeld: transcript, 27–46.

Horn, Nikolai/Stecher, Björn (2019): Denkimpuls innovativer Staat: Datensouveränität – Datenschutz neu verstehen. Initiative D21 – Arbeitsgruppe Innovativer Staat, Stand: 16. Mai 2019. Berlin: Initiative D21. https://initiatived21.de/app/uploads/2019/05/denkimpuls_datenschutz_neu_verstehen.pdf [15.3.2022].

Hornung, Gerrit/Spiecker gen. Döhmann, Indra (2019): Einleitung. In: Simitis, Spiros/dies. (Hg.): Datenschutzrecht – DSGVO mit BDSG. Baden-Baden: Nomos 2019, Rn. 207–310.

Houben, Daniel/Prietl, Bianca (Hg.) ([2]2018): Datengesellschaft. Einsichten in die Datafizierung des Sozialen. Bielefeld: transcript.

Hummel, Patrik/Braun, Matthias/Augsberg, Steffen/Dabrock, Peter (2018): Sovereignty and Data Sharing. In: ITU Journal: ICT Discoveries, Special Issue 2 (2018). https://www.itu.int/en/journal/002/Documents/ITU2018-11.pdf [12.03.2022].

Hummel, Patrik/Braun, Matthias/Dabrock, Peter (2019): Data Donations As Exercises Of Sovereignty. In: Krutzinna, Jenny/Floridi, Luciano (Hg.): The Ethics of Medical Data Donation. Heidelberg/New York: Springer Open, 23–54.

Hummel, Patrik/Braun, Matthias/Augsberg, Steffen/von Ulmenstein, Ulrich/Dabrock, Peter (2021a): Datensouveränität: Governance-Ansätze für den Gesundheitsbereich. Heidelberg/New York: Springer Open. https://link.springer.com/book/10.1007/978-3-658-33755-1 [16.03.2022].

Hummel, Patrick/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021b): Data sovereignity: A review. In: Big Data & Society Vol. 8, Issue 1 2021, 1–17. https://doi.org/10.1177/2053951720982012 [15.3.2022].

Hunzinger, Sven (2018): Das Löschen im Datenschutzrecht. Baden-Baden: Nomos.

Hutt, William H. (1936): Economists and the Public: A Study of Competition and Opinion. London: Jonathan Cape (Reprint (1990): New Brunswick: Transaction Publishers).

Hutt, William H. (1940): The Concept of Consumers' Sovereignty. In: Economic Journal 50(197), 66–77.

Ilgner, Klaus (Hg.) (2021): VDE Position Paper: Technological Sovereignty: Methodology and Recommendations. Frankfurt am Main: VDE – Informationstechnische Gesellschaft (ITG).

Irion, Kristina (2012): Government cloud computing and national data sovereignty. In: Policy & Internet 4(3-4), 40–71.

Iser, Matthias (2009): Kolonialisierung. In: Brunkhorst, Hauke/Kreide, Regina/Lafont, Cristina (Hg.): Habermas Handbuch, Stuttgart/Weimar: Metzler, 328–331.

Itami, Hiroyuki (1987): Mobilising Invisible Assets. Cambridge: Harvard University Press.

Jandt, Silke (2021): Gesetzentwurf für ein Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG-E). In: Datenschutz-Berater 3, 66–69.

Janović, Inga (2021): Rechenzentren als Heizung. In: FAZ-online vom 26.04.2021. https://www.faz.net/aktuell/rhein-main/energiepolitik-wie-rechenzentren-als-heizung-fungieren-soll-17313513.html [28.02.2022].

Jarass, Hans (1989): Das Allgemeine Persönlichkeitsrecht im Grundgesetz. In: Neue Juristische Wochenschrift (NJW) 42, 857–862.

Jarass, Hans ([4]2021): Charta der Grundrechte der Europäischen Union – Kommentar. München: Beck.

Jentzsch, Nicola (2019): Datenhandel und Datenmonetarisierung: Ein Überblick. In: Stiftung Datenschutz (Hg.): Dateneigentum und Datenhandel. Berlin: Erich Schmidt, 177–190.

Jin, Xiaolong/Wah, Benjamin W./Cheng, Xuequi/Wang, Yuanzhuo (2015): Significance and challenges of big data research. In: Big Data Research 2, 59–64.

Jörke, Dirk (2016): Über die Restauration – oder Wege aus der Arendt-Falle. In: Demirović, Alex (Hg.): Transformation der Demokratie – demokratische Transformation. Münster: Westfälisches Dampfboot, 201–224.

Jörke, Dirk (2017): Moralismus ist zu wenig. Kommentar zu Jan-Werner Müllers Essay »Was ist Populismus?«. In: Zeitschrift für Politische Theorie 7(2), 203–208.

Jörke, Dirk/Selk, Veith (2015): Der hilflose Antipopulismus. In: Leviathan 43(4), 484–499.

Jorzig, Alexandra/Sarangi, Frank (2020): Digitalisierung im Gesundheitswesen. Ein kompakter Streifzug durch Recht, Technik und Ethik. Berlin: Springer Nature.

Jurkevics, Anna (2017): Hannah Arendt reads Carl Schmitt's The Nomos of the Earth: a dialogue on law and geopolitics from the margins. In: European Journal of Political Theory 16(13), 345–366.

Kant, Immanuel (1795, $^{2}$1796): Zum ewigen Frieden. Ein philosophischer Entwurf. In: Schriften zur Anthropologie, Geschichtsphilosophie, Politik und Pädagogik 1, Werkausgabe Bd. XI. Frankfurt am Main: Suhrkamp 1977, 191–251.

Kaulartz, Markus (2016a): Rechtliche Grenzen bei der Gestaltung von Smart Contracts. In: Taeger, Jürgen (Hg.): Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Tagungsband Herbstakademie 2016. Edewecht: Oldenburger Verlag für Wirtschaft, Informatik und Recht, 1023–1039.

Kaulartz, Markus (2016b): Herausforderungen bei der Gestaltung von Smart Contracts. In: Zeitschrift zum Innovations- und Technikrecht 2016, 201–206.

Kelsen, Hans ($^{2}$1928): Das Problem der Souveränität und die Theorie des Völkerrechts: Beitrag zu einer Reinen Rechtslehre. Aachen: Scientia 1981.

Kelsen, Hans ($^{2}$1960): Reine Rechtslehre. Mit einem Anhang: Das Problem der Gerechtigkeit. Wien: Deuticke.

Kelsen, Hans (1979): Allgemeine Theorie der Normen (Hg.: Ringhofer, Kurt/Walter, Robert). Wien: Manz.

Kepper, Martina (2016): Hellenistische Bildung im Buch der Weisheit. Studien zur Sprachgestalt und Theologie der Sapientia Salomonis. Berlin/Boston: De Gruyter.

Kerber, Wolfgang (2014): Soft Paternalismus und Verbraucherpolitik. In: List Forum für Wirtschafts- und Finanzpolitik 40(2), 274–295.

Kerber, Wolfgang (2016): Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection. In: Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int.) 65(7), 639–647.

Kerber, Wolfgang (2018): Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data. In: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 9(3), 310–331.

Kerber, Wolfgang (2022): Specifying and Assigning »Bundles of Rights« on Data: An Economic Perspective. In: Hofmann, Franz/Raue, Benjamin/Zech, Herbert (Hg.): Eigentum in der digitalen Gesellschaft, 151–176. http://dx.doi.org/10.2139/ssrn.3847620 [Im Erscheinen].

Kerber, Wolfgang/Vanberg, Viktor (2001): Constitutional Aspects of Party Autonomy and Its Limits – The Perspective of Constitutional Economics. In: Grundmann, Stefan/

Kerber, Wolfgang/Weatherill, Stephen (Hg.): Party Autonomy and the Role of Information in the Internal Market. Berlin und New York: De Gruyter, 49–79.

Kerber, Wolfgang/Gill, Daniel (2020): Datenzugang und Datenschutz im vernetzten Fahrzeug: eine ökonomische Perspektive. In: Stiftung Datenschutz (Hg.): Datenschutz im vernetzten Fahrzeug. Berlin: Erich Schmidt, 85–98.

Kerber, Wolfgang/Specht-Riemenschneider, Louisa (2021): Synergies Between Data Protection Law and Competition Law, Report for the German consumer association Verbraucherzentrale Bundesverband (vzbv). Berlin: vzbv. https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf [25.3.2022].

Kerber, Wolfgang/ Zolna, Karsten K. (2022): The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law. In: European Journal of Law & Economics. https://link.springer.com/article/10.1007/s10657-022-09727-8.

Kersting, Wolfgang ([3]2007): Wohlgeordnete Freiheit. Immanuel Kants Rechts- und Staatsphilosophie. Paderborn: Mentis.

Kettner, Sara Elisa/Thorun, Christian/Spindler, Gerald (2020): Innovatives Datenschutzeinwilligungsmanagement – Abschlussbericht. https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1 [25.3.2022].

Kilian, Wolfgang (2002): Report – Informationelle Selbstbestimmung und Marktprozesse. Zur Notwendigkeit der Modernisierung des Modernisierungsgutachtens zum Datenschutzrecht. In: Computer und Recht (CR), 921–932.

Kingreen, Thorsten (2022): EU-GRCharta Art. 8 Schutz personenbezogener Daten. In: Callies, Christian/Ruffert, Matthias (Hg.): EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta – Kommentar. München: Beck [6]2022, Rn. 1–19.

Klement, Jan Henrik (2017): Öffentliches Interesse an Privatheit. In: Juristenzeitung (JZ) 72, 161–170.

Klement, Jan Henrik (2019): Artikel 7 Bedingungen für die Einwilligung. In: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra, (Hg.): Datenschutzrecht. Baden-Baden: Nomos.

Klug, Petra/Große Starmann, Carsten (2019): Kommunal. Digital. Vernetzt. In: Stubbe, Julian/Schaad, Samer/Ehrenberg-Illies, Simone: Digital souverän? Kompetenzen für ein selbstbestimmtes Leben im Alter. Gütersloh: Bertelsmann, 12–13. https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Smart_Country/Digitale_Souveraenitaet_2019_final.pdf [5.2.2022].

Kluge, Friedrich ([25]2011): Etymologisches Wörterbuch der deutschen Sprache. Berlin/Boston: De Gruyter.

Knorre, Susanne/Müller-Peters, Horst/Wagner, Fred (2020): Die Big-Data-Debatte. Wiesbaden: Springer Fachmedien.

Kokolakis, Spyros (2015): Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. In: Computers & Security 64, 122–134.

Kommission Wettbewerbsrecht 4.0 (2019): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft – Bericht der Kommission Wettbewerbsrecht 4.0, September 2019. https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4 [25.3.2022].

Koot, Martijn/Wijnhoven, Fons (2021): Usage impact on data center electricity needs. A system dynamic forecasting model. In: Applied Energy 291. https://research.utwente.nl/en/publications/usage-impact-on-data-center-electricity-needs-a-system-dynamic-fo [25.3.2022].

Krämer, Jan (2020): Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations. In: Journal of Competition Law & Economics. doi:10.1093/joclec/nhaa030.

Kramme, Malte (2015): Die Einbeziehung von Pflichtinformationen in Fernabsatz- und Außergeschäftsraumverträge. In: Neue Juristische Wochenschrift 59, 279–284.

Krempl, Stefan (2015): IT-Gipfel: Gabriel plädiert für Datensouveränität statt Datenschutz. Heise online 19.11.2015. https://www.heise.de/newsticker/meldung/IT-Gipfel-Gabriel-plaediert-fuer-Datensouveraenitaet-statt-Datenschutz-2966141.html [15.3.2022].

Kretschmer, Tobias (2018): Innovation und Datenschutz. Von datenbasierten Geschäftsmodellen und deren Chancen und Gefahren. In: Wirtschaftsdienst 98(7), 459–462.

Krüger, Philipp-L. (2016): Datensouveränität und Digitalisierung. Probleme und rechtliche Lösungsansätze. In: Zeitschrift für Rechtspolitik 2016, 190–192.

Kühling, Jürgen (2014): Die Europäisierung des Datenschutzrechts. Gefährdung deutscher Grundrechtsstandards? Baden-Baden: Nomos.

Kühling, Jürgen (2020): Gesundheitsdatenschutzrecht im Zeitalter von »Big Data«. Zeit für eine Neukonzeption nach den Vorschlägen des Ethikrates zur Sicherung einer »Datensouveränität«? In: Datenschutz und Datensicherheit, 182–188.

Kühling, Jürgen (2021): Der datenschutzrechtliche Rahmen für Datentreuhänder, Zeitschrift für Digitalisierung und Recht 1 (2021), 1–26.

Kühling, Jürgen/Buchner, Benedikt ($^{3}$2020): DS-GVO BDSG. München: Beck.

Kukutai, Tahu/Taylor, John (2016): Indigenous Data Sovereignty: Toward an agenda. Canberra: ANU Press.

Lahusen, Benjamin (2021): Verdinglichung durch Datenschutz, In: Archiv für die civilistische Praxis 2021, 1–31.

Lambiotte, Renaud/Kosinski, Michal (2014): Tracking the Digital Footprints of Personality. In: Proceedings of the IEEE 102(12): 1934–1939.

Laney, Douglas B. (2018): Infonomics. How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage. New York/Oxon: Bibliomotion.

Lanier, Jaron (2021): Daten-Genossenschaften statt Daten-Eigentum, in: Tagesspiegel Background, 25.01.2021. Online: https://background.tagesspiegel.de/digitalisierung/daten-genossenschaften-statt-daten-eigentum [12.03.2022].

Larenz, Karl (1979): Richtiges Recht. München: C.H. Beck.

Lassalle, Ferdinand (1919): Das Arbeiter-Programm. Über den besonderen Zusammenhang der gegenwärtigen Geschichtsperiode mit der Idee des Arbeiterstandes. Vortrag

vom 12. April 1862. In: Gesammelte Reden und Schriften, herausgegeben von Eduard Bernstein, Bd. 2. Berlin: Paul Cassirer, 147–202.

Leeb, Christina-Maria/Liebhaber, Johannes (2018): Grundlagen des Datenschutzrechts, Juristische Schulung 58, 534–538.

Lerner, Abba P. (1972): The Economics and Politics of Consumer Sovereignty. In: The American Economic Review (AER) 62(2), 258–266.

Leyens, Patrick/Schäfer, Hans-Bernd (2010): Inhaltskontrolle allgemeiner Geschäftsbedingungen. Rechtsökonomische Überlegungen zu einer einheitlichen Konzeptio von BGB und DCFR. In: Archiv für die civilistische Praxis 2010, 771–803.

Lobo, Sascha (2014): Was wirklich hinter der massenhaften Überwachung steckt. SPIEGEL-ONLINE vom 02.07.2014. https://www.spiegel.de/netzwelt/netzpolitik/ueberwachung-und-kontrollwahn-dahinter-steckt-kybernetik-a-978704.html [28.02.2022].

Luch, Anika/Schulz, Sönke/Kuhlmann, Florian (2014): Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit – Anmerkung zum Urteil des EuGH v. 13.5.2014 (Google), Rs. C131/12. In: Zeitschrift Europarecht, 698–715.

Lüde, Rolf von/Moldt, Daniel/Valk, Rüdiger (Hg.) (2009): Selbstorganisation und Governance in künstlichen und sozialen Systemen. Münster: LIT.

Luguri, Jamie/Strahilevitz, Lior Jacob (2021): Shining a Light on Dark Patterns. In: Journal of Legal Analysis 13, 43–109.

Luth, Hanneke A. (2010): Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited. Antwerpen: Intersentia.

Mantz, Reto ($^2$2018): Art. 25. In: Sydow, Gernot (Hg.): Europäische Datenschutzgrundverordnung. Baden-Baden: Nomos.

Marquard, Odo (1994): Skepsis und Zustimmung. Philosophische Studien. Stuttgart: Reclam.

Marquard, Odo (2000): Philosophie des Stattdessen. Studien. Stuttgart: Reclam.

Martini, Mario/Drews, Christian/Seeliger, Paul/Weinzierl, Quirin (2021): Dark Patterns. Phänomenologie und Antworten der Rechtsordnung. In: Zeitschrift für Digitalisierung und Recht 1, 47–74.

Martini, Mario/Kolain, Michael/Neumann, Katja/Rehorst, Tobias/Wagner, David (2021): Datenhoheit. In: Multimedia und Recht (MMR) 24 (Beilage), 3–23.

Martini, Mario/Weinzierl, Quirin (2019): Mandated Choice: der Zwang zur Entscheidung auf dem Prüfstand von Privacy by Default (Art. 25 Abs. 2 S. 1 DSGVO). In: Zeitschrift für rechtswissenschaftliche Forschung 10, 287–316.

Marx, Karl (1962): Das Kapital. Kritik der politischen Ökonomie, Bd. 1/I, Der Produktionsprozeß des Kapitals. In: Karl Marx/Friedrich Engels, Werke Bd. 23. Berlin: Dietz.

Maus, Ingeborg (1980): Bürgerliche Rechtstheorie und Faschismus. Zur sozialen Funktion und aktuellen Wirkung Carl Schmitts. München: Fink.

Maus, Ingeborg (1994): Zur Aufklärung der Demokratietheorie. Rechts- und demokratietheoretische Überlegungen im Anschluß an Kant. Frankfurt am Main: Suhrkamp.

Maus, Ingeborg (2011): Über Volkssouveränität. Elemente einer Demokratietheorie, Berlin: Suhrkamp.

Mayer-Schönberger, Viktor (2012): Was uns Mensch sein lässt – Anmerkungen zum Recht auf Vergessen. In: Datenschutz Nachrichten 35(1), 9–11.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013; [3]2017): Big Data. Die Revolution, die unser Leben verändern wird. München: Redline.

Meinel, Christoph (2020): Deutschland gibt seine Souveränität am Router ab. In: FAZ vom 5.10.2020. https://www.faz.net/aktuell/wirtschaft/digitec/deutschland-gibt-seine-souveraenitaet-am-router-ab-16985236.html [2.5.2022].

Merkel, Angela (2020): Rede zur deutschen EU-Ratspräsidentschaft vor dem Europäischen Parlament am 8. Juli 2020. Berlin: Bundesregierung, 1–11. https://www.bundesregierung.de/breg-de/aktuelles/rede-von-bundeskanzlerin-merkel-zur-deutschen-eu-ratspraesidentschaft-2020-vor-dem-europaeischen-parlament-am-8-juli-2020-in-bruessel-1767368 [5.2.2022].

Mertz, Marcel u.a. (2016): Digitale Selbstbestimmung. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln. https://kups.ub.uni-koeln.de/6891/1/ceres_Digitale_Selbstbestimmung.pdf [28.02.2022].

Meyer, Lukas H. (2005): Historische Gerechtigkeit. Berlin/New York: De Gruyter.

Ministery of Transport and Communications (2015): MyData. A Nordic model for human-centered personal data management and processing. Whitepaper https://julkaisut.valtioneuvosto.fi/handle/10024/78439 [9.3.2022].

Misterek, Fokko (2017): Digitale Souveränität. Technikutopien und Gestaltungsansprüche demokratischer Politik. MPIfG Discussion Paper 17/11. https://pure.mpg.de/rest/items/item_2452828/component/file_2452826/content [25.3.2022].

Möslein, Florian (2011): Dispositives Recht. Tübingen: Mohr Siebeck.

Möslein, Florian (2019a): BGB § 145 Bindung an den Antrag. In: Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph (Hg): Beck-online. Grosskommentar, München: Beck.

Möslein, Florian (2019b): Smart Contracts im Zivil- und Handelsrecht. In: Zeitschrift für das gesamte Handels- und Wirtschaftsrecht 183, 254–293.

Möslein, Florian (2020): Die normative Kraft des Ethischen – ein Fallbeispiel zur Effektivität von Leitlinien zur Künstlichen Intelligenz. In: Recht digital (RDi) 1, 34–41.

Möslein, Florian (2021a): Elektronische Geschäftsanteile. In: Omlor, Sebastian/Möslein, Florian/Grundmann, Stefan (Hg.): Elektronische Wertpapiere. Tübingen: Mohr Siebeck Verlag, 179–206.

Möslein, Florian (2021b): Rechtsgeschäfte unter Abwesenden: Vertragsschluss und Beschlussfassung trotz »Social Distancing«. In: Juristische Ausbildung 43, 1001–1012.

Möslein, Florian (2022): § 1 eWpG. In: von Buttlar, Julia/Segna, Ulrich/Voß, Thorsten (Hg.): Gesetz über elektronische Wertpapiere. München: Beck.

Musielak, Hans-Joachim (2017): Vertragsfreiheit und ihre Grenzen. In: Juristische Schulung 57, 949–954.

Myers West, Sarah (2019): Data Capitalism. Redefining the Logics of Surveillance and Privacy. In: Business & Society 58(1), 20–41.

Neuenschwander, Markus P. (2006): Überprüfung einer Typologie der Klassenführung. In: Schweizerische Zeitschrift für Bildungswissenschaften 28(2), 243–258.

Neuner, Jörg (2022): Die Grundpfeiler der Privatautonomie: Handlungs-, Willens- und Entscheidungsfreiheit. In: Selbstbestimmung: Freiheit und Grenzen Festschrift für Reinhard Singer zum 70. Geburtstag. Berlin: Berliner Wissenschafts-Verlag, 472–486.

Nickel, Philip J. (2019): The Ethics of Uncertainty for Data Subjects. In: Krutzinna, Jenny/ Floridi, Luciano (Hg.): The Ethics of Medical Data Donation. Cham: Springer, 55–74.

Niesen, Peter (2001): Volk-von-Teufeln-Republikanismus: Zur Frage nach den moralischen Ressourcen der liberalen Demokratie. In: Wingert, Lutz/Günther, Klaus (Hg.): Die Öffentlichkeit der Vernunft und die Vernunft der Öffentlichkeit. Festschrift für Jürgen Habermas. Frankfurt am Main: Suhrkamp, 568–604.

Niesen, Peter (2002): Legitimität ohne Moralität. Habermas und Maus über das Verhältnis zwischen Recht und Moral. In ders./Schomberg, René von (Hg.): Zwischen Recht und Moral. Neuere Ansätze der Rechts- und Demokratietheorie. Hamburg/Münster: LIT, 16–60.

Niesen, Peter (2019): Reframing civil disobedience: Constituent power as a language of transnational protest. In: Journal of International Political Theory 15: 1, 31–48.

Niesen, Peter/Eberl, Oliver ([2]2009): Demokratischer Positivismus: Habermas und Maus. In: Buckel, Sonja/Christensen, Ralph/Fischer-Lescano, Andreas (Hg.): Neue Theorien des Rechts. Stuttgart: UTB, 3–26.

Norberg, Patricia A./Horne, Daniel R./Horne, David A. (2007): The privacy paradox: Personal information disclosure intentions versus behaviors. In: Journal of Consumer Affairs 41(1), 100–126.

OECD (2010): Consumer Policy Toolkit. https://read.oecd.org/10.1787/9789264079663-en?format=pdf [25.3.2022].

OECD (2020): Consumer Data Rights and Competition – Background note. https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [25.3.2022].

Ogorek, Markus (2020): Zustimmung zur Speicherung von Cookies. In: Juristische Arbeitsblätter (JA), 478–480.

Otto, Boris (2022): Was ist GAIA-X? In: Digitalgespräch (Podcast) vom 08.02.2022. https://zevedi.de/digitalgespraech-017-boris-otto/ [15.3.2022].

Otto, Boris/Burmann, Anja (2021): Europäische Dateninfrastrukturen Ansätze und Werkzeuge zur Nutzung von Daten zum Wohl von Individuum und Gemeinschaft. In: Informatik Spektrum (44) 2021, 283–291.

Paal, Boris (2020): Marktmacht im Daten(schutz)recht. In: Zeitschrift für Wettbewerbsrecht (ZWeR) (2020)2, 215–244.

Paracelsus (1928): Sieben Defensiones. In: Theophrast von Hohenheim gen. Paracelsus: Sämtliche Werke, herausgegeben von Karl Sudhoff, Abt. 1, Medizinische, naturwissenschaftliche und philosophische Schriften, herausgegeben von Karl Sudhoff, Bd. 11, Schriftwerk aus den Jahren 1537–1541. München/Berlin: Oldenbourg, 123–160.

Parlamentarischer Beirat für nachhaltige Entwicklung des Deutschen Bundestages, Digitalisierung und Nachhaltigkeit Positionspapier (Ausschussdrucksache 19(26)39, 13.09.2019). https://t1p.de/vanp [28.02.2022].

Passow, Franz ([3]1825): Johann Gottlob Schneiders Handwörterbuch der Griechischen Sprache Bd. 2. Leipzig: Vogel.

Peeters, Remi (2009): Truth, Meaning and the Common World: The Significance and Meaning of Common Sense in Hannah Arendt's Thought, Part One. In: Ethical Perspectives 16(3), 337–359.

Peilert, Andreas (2017): BVerfGE 65, 1 – Volkszählung – Das Recht auf informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts. In: Menzel, Jörg/Müler-Terpitz, Ralf/Ackermann, Thomas (Hg.): Verfassungsrechtsprechung. Tübingen: Mohr Siebeck [3]2017, 371–379.

Peitz, Martin/Schweitzer, Heike (2018): Ein neuer europäischer Ordnungsrahmen für Datenmärkte? In: Neue Juristische Wochenschrift (NJW) 62, 275–280.

Persky, Joseph (1993): Retrospectives: Consumer Sovereignty. In: Journal of Economic Perspectives 7, 183–191.

Person, Christian/Schütrumpf, Moritz (2022): Das Projekt Gaia-X – Next Generation einer föderierten Dateninfrastruktur. https://zevedi.de/wp-content/uploads/2022/03/ZEVEDI_Handreichung-Gaia-X_V1.0.pdf [15.3.2022].

Pfeifer, Wolfgang (1989): Etymologisches Wörterbuch des Deutschen. Berlin: Akademie.

Pistor, Katharina (2020): Rule by Data: The End of Markets? In: Law and Contemporary Problems 83, 101–124. https://scholarship.law.duke.edu/lcp/vol83/iss2/6 [25.3.2022].

Plath, Kai-Uwe (2018): Art. 7 DSGVO. In: Plath, Kai-Uwe: DSGVO BDSG, Köln [3]2018.

Podszun, Rupprecht (2020): Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der »Facebook«-Entscheidung des BGH. In: Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 122(12), 1268–1276.

Pohle, Julia (2020a): Digitale Souveränität. In: Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hg.): Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden: Springer VS.

Pohle, Julia (2020b): Digitale Souveränität. Ein neues politisches Schlüsselkonzept in Deutschland und Europa. Konrad Adenauer Stiftung. https://www.kas.de/documents/252038/7995358/Digitale+Souver%C3%A4nit%C3%A4t.pdf/c04017b5-11d6-94b5-5e50-ce9 f71829b1e?version=1.0&t=1608034330280 [5.2.2022].

Pohle, Julia/Thiel, Thorsten (2019a): Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses, 1–20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435002 [5.2.2022].

Pohle, Julia/Thiel, Thorsten (2019b): Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses. In: Borucki, Isabelle/Schünemann, Wolf J. (Hg.): Internet und Staat. Perspektiven auf eine komplizierte Beziehung. Baden-Baden: Nomos, 57–80.

Pohle, Julia/Thiel Thorsten (2021): Digitale Souveränität. Von der Karriere eines einenden und doch problematischen Konzepts. In: Piallat, Chris (Hg): Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt. Bielefeld: transcript, 319–340. DOI: 10.14361/9783839456590-014.

Pohle, Julia/Thiel, Thorsten (2022): Digital Sovereignty. In: Herlo, Bianca u.a. (Hg.): Practicing Sovereignty. Digital Involvement in Times of Crises. Bielefeld: transcript, 47–68.

Püschel, Florian (2014): Big Data und die Rückkehr des Positivismus. Zum gesellschaftlichen Umgang mit Daten. In: Mediale Kontrolle 3(1), 1–23.

Putnings, Markus (2021): Datenökosystem. In: Putnings, Markus/Neuroth, Heike/Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement. Berlin/Boston: De Gruyter, 7–10.

PwC (2019): Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Stand: 23. August 2019. Eine Studie im Auftrag des Bundesministeriums des Innern, für Bau und Heimat. Berlin: PwC. https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf;jsessionid=3430D56EAC931DC35B6909A71AD4BA88.2_cid332?__blob=publicationFile [15.3.2022].

Quartisch, Helmuth (1995): Art. »Souveränität«. In: Ritter, Joachim/Gründer, Karlfried (Hg.): Historisches Wörterbuch der Philosophie Bd. 9: Se-Sp. Basel: Schwabe, 1104–1109.

Rainie, Stephanie Carroll/Schultz, Jennifer Lee/Briggs, Eileen u.a. (2017): Data as a Strategic Resource: Self-determination, Governance, and the Data Challenge for Indigenous Nations in the United States. In: The International Indigenous Policy Journal 8, 1–29. https://repository.arizona.edu/handle/10150/624737?show=full [30.3.2022].

Rat für Digitale Ökologie (2021): 100 Tage Programm für eine nachhaltige Digitalpolitik. https://ratfuerdigitaleoekologie.org/images/downloads/RD%C3%96-Positionspapier-zur-Bundestagswahl.pdf [9.3.2022].

RfII (= Rat für Informationsinfrastrukturen) (2019): Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel. Göttingen: RfII. https://rfii.de/download/herausforderung-datenqualitaet-november-2019 [28.02.2022].

RfII (2020): Stellungnahme: Datentreuhandstellen gestalten – Zu Erfahrungen der Wissenschaft. Göttingen: RfII. https://www.rdm.kit.edu/downloads/RfII-Stellungnahme_Datentreuhand_2020.pdf [19.3.2022].

Reinhardt, Rudolf (1957): Die Vereinigung subjektiver und objektiver Gestaltungskräfte im Vertrage. In: Festschrift zum 70. Geburtstag von Walter Schmidt-Rimpler. Karlsruhe: C.F. Müller, 115–138.

Richter, Heiko (2021): Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine »Verordnung über europäische Daten-Governance«. In: Zeitschrift für Europäisches Privatrecht 28, 634–667.

Riedesel, Jamie (2021): Software Telemetry Reliable Logging and Monitoring. Shelter Island: 2021.

Riehm, Thomas (2020): Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation Daten als Gegenleistung? In: Pertot, Tereza (Hg.): Rechte an Daten. Bayreuth: Mohr Siebeck, 175–206.

Riehm, Thomas (2021): Totgesagte leben länger? 20 Jahre elektronische Form im BGB. In: Festschrift für Johannes Hager zum 70. Geburtstag am 09.07.2021. Berlin: Duncker & Humblot Verlag, 71–94.

Rittel, Claudia Isabel (2021): Rechenzentrum versorgt Neubauquartier Westville mit Wärme. In: Frankfurter Rundschau online vom 08.07.2021. https://www.fr.de/frankfurt/frankfurt-die-waerme-von-nebenan-90850547.html [28.02.2022].

Robertson, Viktoria H.S.E (2020): Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data. In: Common Market Law Review 57, 161–190.

Rosenfeld, Sophia (2011): Common Sense. A Political History. Cambridge/London: Harvard University Press.

Roßnagel, Alexander (2017): § 1 Einleitung: Das künftige Datenschutzrecht nach Geltung der Datenschutz-Grundverordnung. In: Ders. (Hg.): Europäische Datenschutz-Grundverordnung. Baden-Baden: Nomos 2017, Rn. 1–54.

Rückert, Christian (2020): Strafrecht. In: Maume, Philipp/Maute, Lena (Hg.): Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings. München: Beck, 527–604.

Sachverständigenrat für Verbraucherfragen (2017): Gutachten »Digitale Souveränität«, Juni 2017. https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf [9.3.2022].

Sachverständigenrat für Verbraucherfragen (2018): Gutachten »Verbrauchergerechtes Scoring«, Oktober 2018. https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf [9.3.2022].

Sattler, Andreas (2020): Personenbezug als Hindernis des Datenhandels. In: Pertot, Tereza (Hg.): Rechte an Daten. Tübingen: Mohr Siebeck, 49–86.

Schaar, Peter (2010): Privacy by design. In: Identity in the Information Society 3(2), 267–274.

Scharpf, Fabian (2021): Ohne Cookies – Ohne Einwilligung? In: Deutsche Stiftung für Recht und Informatik: Tagungsband Herbstakademie, 379–393.

Schiedermair, Stephanie (2019): IV. 1. b) Grundrechtliche Rahmenbedingungen. In: Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): Datenschutzrecht – DSGVO mit BDSG. Baden-Baden: Nomos 2019, Rn. 161–183.

Schmidt, Jan Cornelius (2004): Auf des Messers Schneide… . Instabilitätstypen in der Nichtlinearen Dynamik. In: Praxis der Naturwissenschaften – Physik 53 (2), 15–21.

Schmidt, Jan Cornelius (2011): The Renaissance of Francis Bacon. In: Nanoethics 5(1), 29–41.

Schmidt, Jan Cornelius (2015): Das Andere der Natur. Neue Wege der Naturphilosophie. Stuttgart: Hirzel.

Schmidt, Jan Cornelius (2021): Technikfolgenabschätzung – und die unterschiedlichen Typen des Wissens. In: Böschen, Stefan/Grunwald, Armin/Krings, Bettina-Johanna/Rösch, Christine (Hg.): Handbuch Technikfolgenabschätzung – ein Orientierungskompass. Nomos: Baden-Baden, 193–208.

Schmidt, Jan Cornelius (2022): Wandel und Kontinuität von Wissenschaft durch KI. Zur aktuellen Veränderung des Wissenschafts- und Technikverständnisse, In: Gethmann, Carl Friedrich u.a. (2022): Künstliche Intelligenz in der Forschung. Neue Möglichkei-

ten und Herausforderungen für die Wissenschaft. Heidelberg/New York: Springer, 79–125.
Schmitt, Carl (1922): Politische Theologie. Vier Kapitel zur Lehre von der Souveränität. Berlin: Duncker & Humblot [7]1996.
Schmitt, Siegfried (2019): Datenintegrität im Pharmaunternehmen. Anforderungen im Arzneimittellebenszyklus berücksichtigen. Schopfheim: GMP.
Schmitz, Barbara / Buschuew Ellen (2022): (Be-)Zahlen mit Daten. In: Multimedia und Recht (MMR) 25 (Beilage), 171–176.
Schneier, Bruce: Data Is a Toxic Asset (2019). In: Schneier, Bruce: We Have Root. Even More Advice from Schneier on Security. Indianapolis: John Wiley & Sons, 211–215.
Schomäcker, Simon (2019): Funktechnik im Bahnverkehr. Störungsfreie Zug-zu-Zug-Kommunikation. Deutschlandfunk vom 07.06.2019. https://www.deutschlandfunk.de/funktechnik-im-bahnverkehr-stoerungsfreie-zug-zu-zug-100.html [28.02.2022].
Schöndorf-Haubold, Bettina (2020): Das Recht auf Achtung des Privatlebens – Grundrechtsschutz in der Informationsgesellschaft. München: Beck.
Schreiber, Gerhard (2022): Im Dunkel der Sexualität. Sexualität und Gewalt aus sexualethischer Perspektive. Berlin/Boston: De Gruyter.
Schüller, Katharina/Busch, Paulina/Hindinger, Carina (2019): Future Skills: Ein Framework für Data Literacy. – Kompetenzrahmen und Forschungsbericht. Arbeitspapier Nr. 47. Berlin: Hochschulforum Digitalisierung. DOI: 10.5281/zenodo.3349865. https://hochschulforumdigitalisierung.de/sites/default/files/dateien/HFD_AP_Nr_47_DALI_Kompetenzrahmen_WEB.pdf [5.2.2022].
Schumacher, Pascal/ Sydow, Lennart/ von Schönfeld, Max (2021): Cookie Compliance, quo vadis? Datenschutzrechtliche Perspektiven für den Einsatz von Cookies und Webtracking nach TTDSG und ePrivacy-VO. In: Multimedia und Recht (MMR) 24, 603–609.
Schwartmann, Rolf/Benedikt, Kristin/Reif, Yvette (2021): Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?. In: Multimedia und Recht (MMR) 24, 99–102.
Schwarz, Kyrill-Alexander (2018): GG Art. 28. In: von Mangoldt, Hermann/Huber, Peter M./Voßkuhle, Andreas (Hg.): Grundgesetz Kommentar. München: Beck [7]2018.
Schwarzkopf, Stefan (2020): Sacred Excess. Organizational Ignorance in an Age of Toxic Data. In: Organization Studies 41(2), 197–217.
Schweitzer, Heike/Peitz, Martin (2017): Datenmärkte: Funktionsweise und Regelungsbedarf. Diskussionspapier 17–43. Mannheim: ZEW.
Schwenke, Matthias Christoph (2006): Individualisierung und Datenschutz. Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung. Wiesbaden: Deutscher Universitäts-Verlag.
Seidel, Ulrich (2014): Das Grundrecht auf Datensouveränität. Notwendige Erweiterung – rechtsökonomische und rechtsstaatliche Auswirkungen. In: Zeitschrift für Gesetzgebung (ZG) 29, 153–165.
Seidel, Ulrich/Seidel, Hendrik (2020): 50 Jahre Datenschutz – wie geht es weiter? In: Zeitschrift für Datenschutz (ZD) 8, 609–610.

Sesing, Andreas (2021): Cookie-Banner – Hilfe, das Internet ist kaputt! In: Multimedia und Recht (MMR) 24, 544–549.

Siciliani, Paolo/Riefa, Christine/Gamper, Harriet (2019): Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making. Oxford: Hart Publishing.

Simitis, Spiros (1987): Programmierter Gedächtnisverlust oder reflektiertes Bewahren. In: Fürst, Walter (Hg.): Festschrift für Wolfgang Zeidler Bd. 2. Berlin: de Gruyter, 1475–1506.

Simitis, Spiros (1994): Die Entscheidung des Bundesverfassungsgerichts zur Volkszählung – 10 Jahre danach. In: Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 77, 121–137.

Simitis, Spiros/Spiecker gen. Döhmann, Indra/Hornung, Gerrit (2019): Datenschutzrecht: DSGVO mit BDGS. Baden-Baden: Nomos.

Simon Assion (2014): Vergesst das Recht auf Vergessenwerden. In: Kappes, Christoph u.a. (Hg.): Medienwandel kompakt 2011 – 2013. Netzveröffentlichungen zu Medienökonomie, Medienpolitik & Journalismus. Wiesbaden: Springer VS, 93–99.

Singer, Reinhard (1995): Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen. München: Beck.

Smart Data Forum (o. J.): Datensouveränität. https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Smart-Data-Forum/wissen-datensouveraenitaet.pdf?__blob=publicationFile&v=2 [29.3.2022].

Solove, Daniel J. (2013): Privacy Self-Management and the Consent Dilemma. In: Harvard Law Review 126, 1880–1903.

Sommer, Manfred (2020): Stift, Blatt und Kant. Philosophie des Graphismus. Berlin: Suhrkamp.

Specht-Riemenschneider, Louisa/Blankertz, Aline (2021): Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken. In: Multimedia und Recht (MMR) 24, 369–370.

Specht-Riemenschneider, Louisa/Blankertz, Aline/Sierek, Pascal/Schneider, Ruben/Knapp, Jakob/Henne, Theresa (2021): Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle. In: Multimedia und Recht (MMR) 24 (Beilage), 25–48.

Specht-Riemenschneider, Louisa/Kerber, Wolfgang (2022): Designing Data Trustees, A purpose-based approach. Datentreuhänder – Ein problemlösungsorientierter Ansatz. Berlin: Konrad-Adenauer-Stiftung. https://www.kas.de/en/single-title/-/content/datentreuhaender-ein-problemloesungsorientierter-ansatz [25.3.2022].

Spindler, Gerald (2021a): Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB Schwerpunkt 2: Rechtsbehelfe, Beweislastregelungen und Regress zwischen Unternehmern. In: Multimedia und Recht (MMR) 24, 528–533.

Spindler, Gerald (2021b): Schritte zur europaweiten Datenwirtschaft – der Vorschlag einer Verordnung zur europäischen Data Governance. In: Computer und Recht (CR) 17, 98–108.

Spitz, Malte (2017): Daten – das Öl des 21. Jahrhunderts? Nachhaltigkeit im digitalen Zeitalter. Hamburg: Hoffmann und Campe.

Staab, Philipp/Piétron, Dominik (2021): Gemeinwohlorientierte Plattformen als Grundlage sozialer Freiheit, in: Piallat, Chris (Hg.): Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt. Bielefeld: transcript, 187–206.

Staab, Philipp/Thiel, Thorsten (2021): Privatisierung ohne Privatismus. Soziale Medien im digitalen Strukturwandel der Öffentlichkeit. In: Seeliger, Martin/Sevignani, Sebastian (Hg.): Ein neuer Strukturwandel der Öffentlichkeit? Leviathan Sonderband 37. Baden-Baden: Nomos, 277–297.

Stäheli, Urs (2021): Soziologie der Entnetzung. Berlin: Suhrkamp.

Stampfl, Nora S. (2012): Leben im digitalen Panopticon. Wie das Internet unsere Wahrnehmung der Welt bestimmt. In: Scheidewege: Jahresschrift für skeptisches Denken 42 (2012/2013), 393–405.

Steinrötter, Björn (2017): Vermeintliche Ausschließlichkeitsrechte an binären Codes. In: Multimedia und Recht (MMR) 20 (Beilage), 731–736.

Stiemerling, Oliver/ Weiß, Steffen /Wendehorst, Christiane (2021): Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, v. 16.12.2021. https://www.ecambria-experts.de/it-sachverstaendiger/wp-content/uploads/2022/01/211216-Gutachten_fuer_Bundesministerium_fuer_Wirtschaft_und_Energie_p-os37621.pdf [30.3.2022].

Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung. https://infoplattform.stiftungdatenschutz.org/themen/pims-studie/ [9.3.2022].

Stoellger, Philipp (2021): Was bedeutet Digitalisierung – für »die« Schrift »als« Schrift? In: Held, Benjamin/Oorschot, Frederike van (Hg.): Digitalisierung: Neue Technik – neue Ethik: Interdisziplinäre Auseinandersetzung mit den Folgen der digitalen Transformation, Heidelberg: heiBOOKs. https://books.ub.uni-heidelberg.de/heibooks/reader/download/945/945-4-95746-2-10-20211109.pdf [16.03.2022].

Stumpf, Felix (2017): Das Recht auf Vergessenwerden. Das Google-Urteil des EuGH. Vorbote der zweiten Chance im digitalen Zeitalter oder Ende der freien Kommunikation im Internet? Marburg: Tectum.

Sunstein, Cass R./Thaler, Richard H. (2003): Libertarian Paternalism Is Not an Oxymoron. In: The University of Chicago Law Review 70(4), 1159–1202.

Taeger, Jürgen (2022). In: Taeger, Jürgen/Gabel, Detlev (Hg.): DSGVO BDSG TTDSG, $^{4}$2022.

Tardieu, Hubert/Otto, Boris (2021): Digital Sovereignty, European Strength and the Data and Cloud Economy – in varietate concordia. In: Revue Européenne du Droit Bd. 2, 12/2021, 98–104.

Thaler, Richard H./Sunstein, Cass R. (2008): Nudge: Improving Decisions About Health, Wealth and Happiness. Yale University Press.

Thiel, Thorsten (2012): Republikanismus und die Europäische Union. Eine Neubestimmung des Diskurses um die Legitimität europäischen Regierens. Baden-Baden: Nomos.

Thiel, Thorsten (2013): Politik, Freiheit und Demokratie: Hannah Arendt und der moderne Republikanismus. In: Schulze Wessel, Julia/Salzborn, Samuel/Volk, Christian (Hg.): Ambivalenzen der Ordnung. Der Staat im Denken Hannah Arendts. Wiesbaden: Springer VS, 259–281.

Thiel, Thorsten (2014): Mehr Arendt wagen: Ja, aber... In: Theorieblog, 05. Februar 2014. https://www.theorieblog.de/index.php/2014/02/mehr-arendt-wagen-ja-aber/ [12.03.2022].

Thiel, Thorsten (2019): Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation, in: Hofmann, Jeanette/Kersting, Norbert/Ritzi, Claudia/Schünemann, Wolf J. (Hg.): Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven. Bielefeld: transcript, 47–60.

Thiel, Thorsten (2021): Das Problem mit der digitalen Souveränität. In: FAZ vom 26. Januar 2021. https://www.faz.net/aktuell/wirtschaft/digitec/europa-will-in-der-informationstechnologie-unabhaengiger-werden-17162968.html [15.3.2022].

Thiele, Ulrich (2008): Die politischen Ideen. Von der Antike bis zur Gegenwart. Wiesbaden: Marix.

Thompson, Michael (2021): Mülltheorie: Über die Schaffung und Vernichtung von Werten (1979). Bielefeld: transcript.

Thouvenin, Florent (2017): Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs. In: Schweizerische Juristen-Zeitung 113 (2017), 21–32.

Thylstrup, Nanna Bonde (2019): Data out of place. Toxic traces and the politics of recycling. In: Big Data & Society 2019 6(2), 1–9.

Tidy, Joe (2022): Ukraine crisis: »Wiper« discovered in latest cyber-attacks. In: BBC News vom 24.02.2022. https://www.bbc.com/news/technology-60500618 [28.02.2022].

Tiedeke, Anna S. (2021): Die (notwendige) Relativität digitaler Souveränität. In: Multimedia und Recht (MMR) 24, 624–628.

TTDSG (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien) (2021). https://gesetz-ttdsg.de/ [25.3.2022].

Uecker, Philip (2019): Die Einwilligung im Datenschutzrecht und ihre Alternativen. In: Zeitschrift für Datenschutz (ZD) 10, 248–251.

Vaile, Daniel (2014): The Cloud and data sovereignty after Snowden. In: Australian Journal of Telecommunications and the Digital Economy 2(1), https://telsoc.org/journal/ajtde-v2-n1/a31 [15.3.2022].

Véliz, Carissa (2021): Privacy is Power. Why and How You Should Take Back Control of Your Data. London: Penguin Random House.

Verbraucherzentrale Bundesverband e.V. (2020): Neue Datenintermediäre, Anforderungen des vzbv an »Personal Information Management Systems« (PIMS) und Datentreuhänder 15.09.2020. https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf [25.3.2022].

Verbraucherzentrale Bundesverband e.V. (2021): Datenschutz und Privatsphäre bei Telekommunikationsdiensten sicherstellen, Stellungnahme des Verbraucherzentrale Bundesverbands zum Referentenentwurf des Bundesministeriums für Wirtschaft und Energie für ein Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG-

E), v. 21.01.2021. https://www.vzbv.de/sites/default/files/downloads/2021/01/22/21-01-21_vzbv-stellungnahme_ttdsg-e.pdf [25.3.2022].
Voigt, Rüdiger (2015): Der moderne Staat. Wiesbaden: Springer Fachmedien.
Von der Leyen, Ursula (2019): A Union that Strives for More. My agenda for Europe. Political Guidelines for the Next European Commission 2019–2024, 16 July 2019. Brüssel: EU. https://op.europa.eu/s/oSKL [5.2.2022].
Von der Leyen, Ursula (2020): State of der Union Address, European Parliament Plenary, 16. September 2020. Brüssel: EU. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 [5.2.2022].
von Ulmenstein, Ulrich (2020): Datensouveränität durch repräsentative Rechtswahrnehmung. Begriffliche Prägung und normative Gestaltung sogenannter »Datentreuhänder«. In: Datenschutz und Datensicherheit 44, 528–534.
Wacket, Julia (2020): Frankfurts Rechenzentren boomen. Tagesschau.de vom 25.09.2020. https://t1p.de/0slwu [28.02.2022].
Wagner, Timo (2019): Verletzungen und Übergriffe: Cyber-Mobbing und andere Formen von Online-Gewalt. In: Grimm, Petra/Kerber, Tobias/Zöllner, Oliver (Hg.): Digitale Ethik. Leben in vernetzten Welten. Ditzingen: Reclam, 121–133.
Welser, Howard T. u.a. (2008): Distilling Digital Traces: Computational Social Science Approaches to Studying the Internet. In: Fielding, Nigel/Lee, Raymond M./Blank, Grant (Hg.): The SAGE Handbook of Online Research Methods. London u.a.: Sage, 116–140.
Wenhold, Céline (2018): Nutzerprofilbildung durch Webtracking. Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen. Baden-Baden: Nomos.
Wiegerling, Klaus/Heil, Reinhard (2019): Ethische Dimensionen der Digitalisierung im Gesundheitswesen. In: GGW 19(3), 15–21.
Wielsch, Dan (2013): Grundrechte als Rechtfertigungsgebote im Privatrecht. In: Archiv für die civilistische Praxis 213, 718–759.
Wilke, Helmut (1983): Entzauberung des Staates. Überlegungen zu einer gesellschaftlichen Steuerungstheorie. Königstein/Taunus: Athenäum.
Wilke, Helmut (2007): Smart Governance. Governing the Global Knowledge Society. Frankfurt am Main, New York: Campus.
Witt, Bernhard C. (2007, $^{2}$2010): Datenschutz kompakt und verständlich. Eine praxisorientierte Einführung. Wiesbaden: Springer.
Wolf, Manfred (1970): Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessensausgleich. Tübingen: Mohr Siebeck.
Zech, Herbert (2012): Information als Schutzgegenstand. Tübingen: Mohr Siebeck.
Zech, Herbert (2015a): »Industrie 4.0« – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. In: Gewerblicher Rechtsschutz und Urheberrecht 2015, 1151–1160.
Zech, Herbert (2015b): Daten als Wirtschaftsgut – Überlegungen zu einem »Recht des Datenerzeugers«. In Computer und Recht (CR) 11, 137–146.
Zech, Herbert (2017): Data as a Tradeable Commodity – Implications for Contract Law. Cambridge: Cambridge University Press.

Zech, Herbert (2020): Besitz an Daten? In: Pertot, Tereza (Hg.): Rechte an Daten. Bayreuth: Mohr Siebeck, 91–102.

Zuboff, Shoshana (2016): Überwachungskapitalismus. Wie wir Googles Sklaven wurden. FAZ vom 05.03.2016. https://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/shoshana-zuboff-googles-ueberwachungskapitalismus-14101816.html [28.02.2022].

Zuboff, Shoshana (2019): The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York: Profile Books.

Zurstiege, Guido (2019): Taktiken der Entnetzung. Die Sehnsucht nach Stille im digitalen Zeitalter. Berlin: Suhrkamp.

# Autorinnen und Autoren

*Steffen Augsberg* ist Professor für Öffentliches Recht an der Justus-Liebig-Universität Gießen.

*Clara Beise* ist Wissenschaftliche Mitarbeiterin in der Arbeitsgruppe für Bürgerliches Recht, Deutsches und Europäisches Wirtschaftsrecht an der Philipps-Universität Marburg.

*Tim Eckes* ist Wissenschaftlicher Mitarbeiter am Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI) sowie im Projekt EuroDaT.

*Kevin Ferber* ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht an der Justus-Liebig-Universität Gießen.

*Stefan Gammel* ist Projektmitarbeiter am Philosophischen Institut der TU Darmstadt und Mitglied des dort angesiedelten nanobüros, dem Büro für interdisziplinäre Nanotechnikforschung.

*Petra Gehring* ist Professorin für Philosophie an der TU Darmstadt.

*Wolfgang Kerber* ist Professor für Wirtschaftspolitik an der Philipps-Universität Marburg.

*Florian Möslein* ist Professor für Bürgerliches Recht, Deutsches und Europäisches Wirtschaftsrecht an der Philipps-Universität Marburg.

*Christian Person* ist Wissenschaftlicher Mitarbeiter am Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI) sowie im Projekt EuroDaT.

*Anne Riechert* ist Professorin für Datenschutzrecht und Recht in der Informationsverarbeitung an der Frankfurt University of Applied Sciences.

*Jan C. Schmidt* ist Professor für Wissenschafts- und Technikphilosophie an der Hochschule Darmstadt.

*Gerhard Schreiber* ist Akademischer Rat am Institut für Theologie und Sozialethik der TU Darmstadt.

*Moritz Schütrumpf* ist Wissenschaftlicher Mitarbeiter in der Arbeitsgruppe für Bürgerliches Recht, Deutsches und Europäisches Wirtschaftsrecht an der Philipps-Universität Marburg.

*Karsten Konrad Zolna* ist Wissenschaftlicher Mitarbeiter in der Arbeitsgruppe für Wirtschaftspolitik an der Philipps-Universität Marburg.